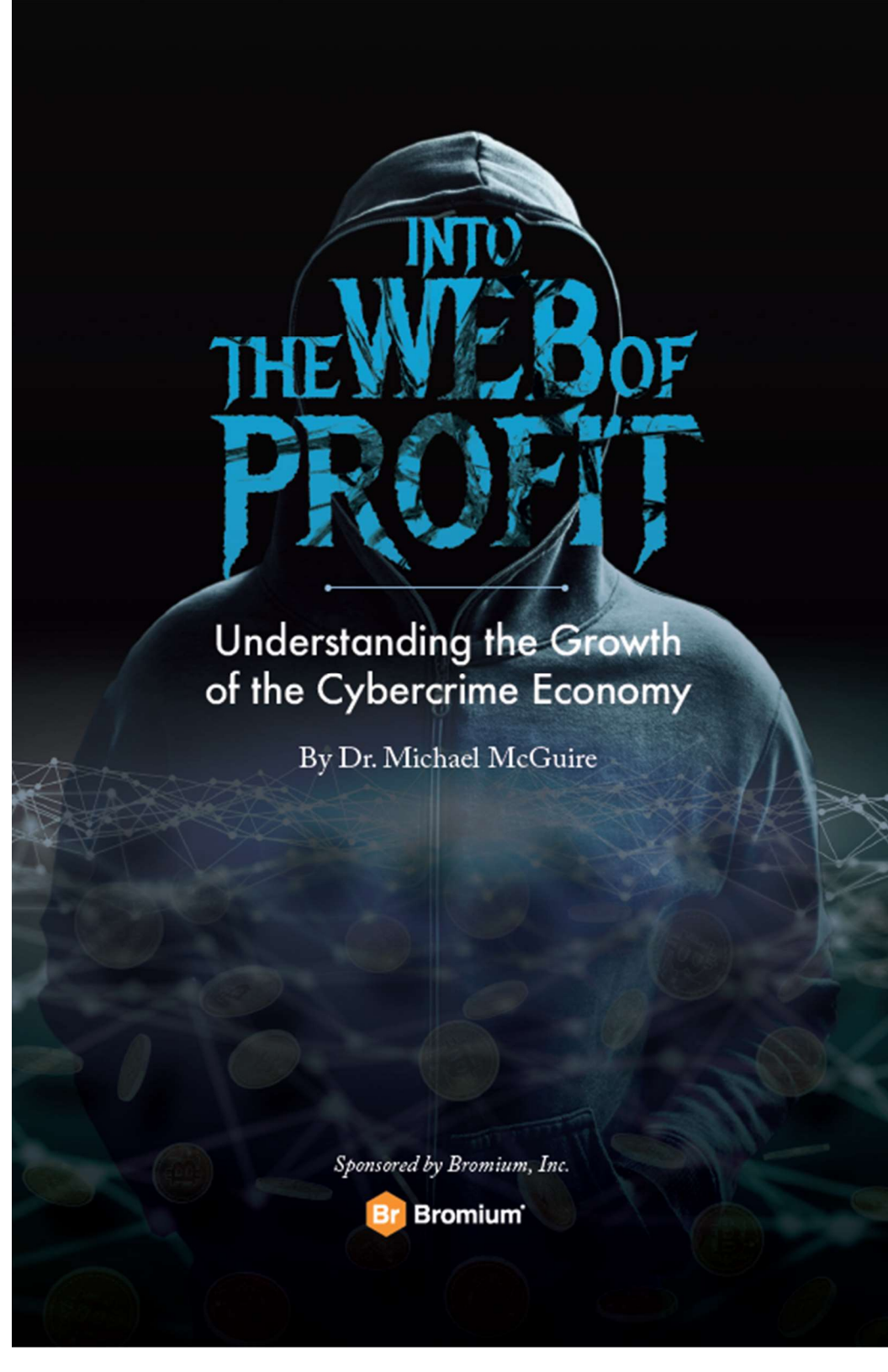


Understanding the Growth of the Cybercrime Economy

By Dr. Michael McGuire

Sponsored by Bromium, Inc.

Bromium

Into The Web of Profit

An in-depth study of cybercrime, criminals and money.

Researched and written by Dr. Mike McGuire
April 2018

Project funded by Bromium, Inc.

Acknowledgements

Many thanks to the various experts from U.S. and European criminal justice agencies, financial institutions and to academic informants who were consulted during the research conducted for this report.

Particular thanks go to the U.K. National Fraud Intelligence Bureau as part of the City of London Police for providing invaluable data and to The National Crime Agency, The Metropolitan Police and the Home Office Cybercrime Research Unit for their helpful suggestions and support.

Table of Contents

Table of Figures

Foreword

Gregory Webb
CEO, Bromium

We invested in this research because we think it's important. The findings of Dr. McGuire's research explain how cybercrime proceeds are being generated, laundered and reinvested into the criminal economy. By gaining a better understanding of the systems that support cybercrime, we think we can better understand how to disrupt them.

Essentially, we want to make life harder for hackers.

Cybercriminals are always one step ahead of the cybersecurity industry; an industry that is generally struggling to fix the problem. Data is a valuable commodity that can be traded and sold – cybercrime is therefore a lucrative business, with relatively low risks compared to other forms of crime. Cybercriminals are rarely convicted. And now that anyone can buy pre-packaged malware and hire hackers-on-demand, it's easier than ever.

In this report, Dr. McGuire has identified the emergence of "platform criminality" – where the cybercrime economy is now

taking the same form as new digital businesses, making it even easier to conduct cyberattacks. They have automated the process so we're likely to see more, frequent attacks.

"It is society that is suffering the consequences of our failure to stem the tide."

The walls between the criminal and legitimate worlds are blurring; we are not simply dealing with 'hackers in hoodies', we are tackling an economic ecosystem that enables, funds and supports criminal activity on a global scale – from drug trafficking to terrorism. It is society that is suffering the consequences of our failure to stem the tide.

The report shows that cybercriminals are both innovators and early adopters of technology. It is unrealistic to think that law enforcement alone will be able to track and disrupt new systems. Because we are a community with a common goal, we need to collaborate and be willing to do things differently. We share a social and moral obligation to disrupt the core systems that underpin this criminal ecosystem.

We need to make it more difficult for hackers to gather our most precious resource – data. The cybersecurity industry needs to come to terms with the limitations of detect-to-protect security and find better ways to isolate the problem. We need to approach cyber-defenses in a totally different way, by focusing on the most vulnerable – and easiest to attack – vectors in our organizations. The criminals know where we are vulnerable – most often where humans put fingers to keyboards. We know changing human behavior is both challenging and costly.

Instead, by focusing on protection, rather than detection, we can disrupt cybercrime in significant ways.

Research is vital to our understanding of cybercrime and may help us one day put an end to The Web of Profit. In the meantime, we will work with our peers to continue to protect the internet and the organizations that rely on it to communicate, collaborate and conduct business.

Let's work together now to disrupt The Web of Profit.

Foreword

Dr. Michael McGuire
Senior Lecturer, University of Surrey

Awareness of cybercrime is at an all-time high, yet understanding of how cybercrime functions as an integrated set of criminal practices remains far less clear. While there is far greater comprehension of the scope and scale of the threat, developed understanding of how cybercrime functions and the factors which drive and support it remains limited.

To date, attention has been primarily focused on the mechanisms of cybercrime – that is, how it happens. As a result, technical factors, such as malware types, security holes and the prevention of certain types of attack, are most frequently discussed. More recently the 'human factor' – that is, the way that human error and poor judgement may contribute to the success of cybercriminals in breaching systems – has begun to be treated more seriously as a causal factor.

However, what remains far less developed is an understanding of cybercrime as a system; one where criminals, victims, policing and security professionals, companies, nation states, financial institutions, service and support mechanisms

interconnect with one another and with various infrastructures (such as data silos, payment systems or even the web itself) to produce a composite whole.

This system is dynamic and evolving and one of its key driving factors is revenue generation and ultimately profit, since this constitutes one of the primary motivations for engaging in cybercrime – or, indeed, crime in general. Understanding revenue generation and its flows not only offers a different way in which our knowledge of cybercrime can be enhanced, but by better understanding revenue structures and their flows, new options can be developed for controlling it.

The Web of Profit project is one of the first major studies to attempt to view the dynamics of cybercrime through the lens of revenue/profit flows. By focusing on developing better understanding of the relevant factors around revenue and profit, the aim has been to contribute to a new kind of knowledge base; one distinct from the largely responsive or 'fire-fighting' strategies that have typified current approaches.

Accordingly, three key factors structure the discussion of the research that follows: how revenues are generated and which revenues are the most lucrative at present; how revenues are being moved around or laundered; and where revenues are spent or converted into other assets or activities.

Introduction

The Emerging Criminal Economy: Cyberspace and The Web of Profit

Financially-driven motivations represent the most important single driver of both the form and spread of cybercrime. Money exerts a more powerful influence upon cybercriminals than earlier motivations, such as the intellectual 'thrill' of penetrating secure computers. However, the (often overused) metaphor of "cybercrime as a business" is no longer adequate to capture its complexities. A more appropriate metaphor is an economy, not a business; a structure functioning as a literal "Web of Profit" – a hyper-connected range of economic agents, economic relationships and other factors now capable of generating, supporting and maintaining criminal revenues at unprecedented scale.

The Web of Profit does not just feed off its legitimate counterpart, it also supports and bolsters revenue generation and profit in the conventional world. The result is a growing interconnectedness and interdependence between them both. Companies and nation states now make money from it, acquire

data and competitive advantages from it, and use it as a tool for strategy, global advancement and social control.

"The cybercrime economy has now become a kind of mirror image of contemporary capitalism."

Equally, if not more significantly, the cybercrime economy has now become a kind of mirror image of contemporary capitalism – reproducing disruptive business models popularised by the likes of Amazon and Uber. As a kind of 'monstrous double' of the legitimate information economy – where data is king – The Web of Profit is not just feeding off the way wealth is generated there, it is reproducing and, in some cases, outperforming it. This is most obviously evident in the platform models of wealth creation it has now adopted.

The complex cybercrime economy that supports The Web of Profit consists of (at least) the following:

- A dizzying range of methods and mechanisms for generating revenues, often at industrial scales.
- Digitally specific currencies and currency exchange tools.
- A range of specialised economic agents, such as producers, suppliers, service providers and consumers.
- The extraction and exchange of data as the key raw material and object of value for illicit trading (this trade now occurs across many dimensions and no longer simply involves buying or selling data from stolen credit or debit cards, but newer data forms that possess value – such as hotel loyalty points, 'likes' on Facebook, account login details and even

soft drink formulas or government-developed hacking tools).

- Dedicated production zones and centres of income generation – whether these be troll factories in Russia, the Hackerville fraud villages in Romania, or mass marketing scam centres in West Africa.
- Specialised tool supply, technical support and provision of skills and expertise.
- Professionalisation and the development of career structures – this includes training, CVs, personal recommendations and references.
- Dedicated marketplaces, not just for obviously illicit items – like drugs, firearms, stolen data or trade secrets – but doppelganger products which, again, mirror commerce within the legitimate economy, in the form of fake goods, fake services, fake authenticity and identity and even fake news.
- Global distribution mechanisms.
- Self-regulation and an alternative rule of law.

In this report, we dissect The Web of Profit, delving specifically into three core functions that make up the broader picture of the cybercrime economy:

- How cybercrime revenues are generated.
- How cybercrime revenues are laundered/transformed.
- How cybercrime revenues are ultimately disposed and reinvested.

Cybercrime Revenues Reach $1.5 Trillion

Though it constitutes a relatively new criminal economy, cybercrime is already generating *at least* $1.5 trillion in revenues every year. This is a conservative estimate, based only on data drawn from five of the highest profile and lucrative varieties of revenue-generating cybercrimes:

Crime	Annual Revenues*
Illicit, illegal online markets	$860 billion
Trade secret, IP theft	$500 billion
Data trading**	$160 billion
Crimeware, CaaS (Cybercrime-as-a-Service)	$1.6 billion
Ransomware***	$1 billion
*totals are approximate **Revenues derived from trading in stolen data, such as: credit and debit card information banking log-in details, loyalty schemes and so on ***Revenues derived from extortions based on encrypting data and demanding payments	

Table 1: Annual Cybercrime Revenue Estimates

Illicit and illegal online markets are now the most lucrative cybercriminal form of revenue generation, constituting over 50% of total revenues, while theft of trade secrets and other IP constitutes around 35% of cybercrime revenues. The use of stolen data as an object of trade and commerce is a vibrant part of the cybercrime economy, constituting around 11% of total revenues. As a lower-risk activity, it may now be more attractive than the original theft itself.

Cybercrime-as-a-Service (CaaS) and ransomware can represent high-yield revenue options for individual

cybercriminals, but represent lower single categories of revenue generation (at present), with each contributing less than 1% of total revenues respectively. Some qualifications are recommended around these estimates: firstly, only three categories of crimeware/CaaS were considered for this estimate, so the real figure is likely to be higher. Secondly, ransomware could be included within the crimeware/CaaS category, since ransomware tools can often be bought or hired on crimeware platforms.

Given its high profile at present, ransomware was treated as a separate category for this research, though its associated revenues may have reached a high point as detection and prevention systems are refined. Certainly, the claim that ransomware represents one of the most lucrative cybercrimes may hold in the case of individual attacks, but the overall revenues remain low in comparison to other categories.

"There is evidence that cybercrime revenues often exceed those of legitimate companies."

Revenues – that is, the gains to be made from engaging in cybercrime – offer a novel, less tested way of understanding these offences than previous financial measures, such as cost or the losses that cybercrime causes. Whilst it is hard to be sure how revenues from cybercrime compare to traditional (purely physical or non-computer-enabled) crime, evidence gathered for this report from both primary and secondary sources indicates that there are a range of crime categories; fraud being perhaps the most obvious example where cybercrime is now the more

profitable form of offending. Not only do the earnings of individual cybercriminals within such categories exceed their counterparts in the traditional crime world, there are far more who are able to engage and earn revenues from it. Thus, whilst total revenue from traditional crime is probably still higher overall, it is by no means clear how long this will continue – especially given the increasing interdependence between cyber and traditional methods, as for example, in counterfeiting.

There is evidence that cybercrime revenues often exceed those of legitimate companies – especially at the small-mid range size. In fact, revenue generation in the cybercrime economy takes place at a variety of levels – from large 'multi-national' operations that can generate profits of over $1 billion; to smaller, small scale operations, where profits of $30,000-$50,000 are more the norm.

Post-Crime and Platform Criminality

The emergence of a complex and multi-layered cybercrime economy has also begun to suggest a fundamental shift in the very nature of crime itself. In this context, overt acts of crime become less central features of the criminal ecosystem when compared to the services and platforms that feed off and support crime – which become increasingly low-investment, high-yield and low-risk operations.

The result is a shift towards platform models of criminality, mirroring shifts in the contemporary global economy that have been characterised as "platform capitalism". This term describes how companies like Uber, Google, Facebook, YouTube, Instagram, LinkedIn and so on are now able to generate

significant revenues merely by offering platforms to others and harvesting their data.

"The result is a shift towards platform models of criminality, mirroring shifts in the contemporary global economy."

In cybercriminal terms, the platform model generates revenues in two forms:

- Exploitation of legitimate platforms
- Creation of new types of illicit platforms

A post-crime world of criminality begins to emerge. This is not one where serious offences like homicide cease to exist or become any less traumatic to victims. Rather, it is one where varieties of criminality that involve less crime, or that take on a secondary form and benefit indirectly, become more attractive in terms of revenue generation.

Both the legitimate and illegitimate economies come together within an increasingly cyber-criminogenic world; one where the tools and cultures of information crime become blurred and interchangeable with the tools and cultures of an information society, and vice versa.

Moving Revenues

As with any criminal endeavour, the increasing profits made from cybercrime require increasingly complex ways of laundering or disposing of them. Around 10% or more of the estimated $1.6-$2 trillion of laundered money being circulated

globally can be attributed to revenues derived from cybercrime – totalling up to $200 billion.

Evidence suggests that cybercriminals have become increasingly adept at deploying traditional methods of laundering, such as: illicit uses of the legitimate banking system, money mules, shell companies, and wire transfers.

Complementing (and sometime used in conjunction with) these are innovative, more digitally-focused methods of laundering, such as the use of online payment systems like PayPal; cryptocurrencies like Bitcoin; or even online gaming currencies.

But the use of cryptocurrencies for laundering purposes has quickly acquired a reputation that far exceeds its actual criminal usage. Best estimates suggest only around 4% of money laundered at present is in Bitcoin or other cryptocurrency forms.

"Both the legitimate and illegitimate economies come together within an increasingly cyber-criminogenic world."

Cryptocurrencies do, however, constitute a major ingredient in the new cybercrime economy, with significant implications for how revenues are likely to be channelled through legal and illegal economies in the future. In this context, Bitcoin is only an entrée to a far more developed world of laundering, utilising a range of new and continually emerging cryptocurrencies.

Transactions using cryptocurrencies are not as anonymous as they have been popularly supposed. The blockchain system, which supports them, generates transparent public records.

Also, evidence has emerged that even when mixer systems are used to further obscure activity, up to 60% of cryptocurrency transactions can be linked to individuals because of other data (such as web cookies) leaking out and leaving traces.

A range of successful operations involving the seizure of cryptocurrency assets have demonstrated the growing skills and capacity of law enforcement to track cryptocurrency transactions.

Disposal of Cybercrime Funds

Utilising interview and observational data of a sample of individuals either convicted, or currently engaged in cybercriminal activities, it emerged that:

- 15% of the cybercriminals sampled spent the majority of their revenues on covering immediate needs – such as buying nappies/diapers or paying bills.
- 20% of the cybercriminals sampled focused the spending of their revenues on disorganised or hedonistic spending – for instance, buying drugs or paying prostitutes.
- 15% of the cybercriminals sampled directed their revenues towards more calculated spending to attain status, or to impress partners and other criminals – for example, buying expensive jewellery.
- 30% of the cybercriminals sampled converted some of their revenues into assets – such as property.
- 20% of the cybercriminals sampled used at least some of their revenues to reinvest in further criminal activities – for example, buying equipment or more crimeware, as well as

channelling revenues to the production of illegal drugs, human trafficking and terrorism.

"Rewards sought by cybercriminals have not changed very much from their traditional counterparts."

These results indicate some interesting structural continuities in the way revenues are used by criminals, suggesting that the rewards sought by cybercriminals have not changed very much from their traditional counterparts.

For example, the research found clear evidence of a continuing penchant for spending profits on luxury goods, such as high-end cars, jewellery and so on. There was also evidence that, like traditional criminals, cybercriminals are willing to transform revenues into longer-term assets, such as property and land, or more unconventional investments, like wine or art.

However, the cybercrime economy presents new options in which assets can be cashed out – such as commodities directly purchasable with cryptocurrencies and other digital payment tools.

Significantly, there was also evidence that revenues are being invested in further cybercrime. This may be in the form of relatively low-level purchases on equipment and tools, or higher-end long-term investments in further crime.

More concerning is evidence that cybercrime revenues are now significant enough to attract the attention of those who are ready to use them to fund more serious crime, such as human trafficking or even terrorism.

At the same time, the developing pressures upon cybercriminals to find ways of achieving the cash out process when using digital proceeds is likely to present new options to law enforcement and cybersecurity professionals for intercepting and disrupting cybercrime.

Metrics: At-A-Glance

Understanding The Web of Profit Through Numbers

Want to skim the highlights of this report? We've tried to make that easy for you. This section provides summaries, visuals and at-a-glance snippets to help you discover information easily.

Crime	Annual Revenues*
Illicit, illegal online markets	$860 billion
Trade secret, IP theft	$500 billion
Data trading**	$160 billion
Crimeware/CaaS (Cybercrime-as-a-Service)	$1.6 billion
Ransomware***	$1 billion
Total Generated by Cybercrime	**$1.5 trillion**

*totals are approximate
**Revenues derived from trading in stolen data, such as: credit and debit card information banking login details, loyalty schemes and so on
***Revenues derived from extortions based on encrypting data and demanding payments

The FBI estimated that ransomware payments in 2016 alone would reach around $1 billion. Revenues from selected ransomware products:

Ransomware	Period	Profit Evaluation
CryptoLocker	2013	~$3 million
Cryptowall	2014-16	~$18-$320 million
Locky		$7.8-$150 million
Cerber		$6.9 million
WannaCry	2016	$55,000-$140,000
Petya/NotPetya		$10,000

Cybercrime Revenue Generation Can be Big or Small

- Large multi-nationals with profits totalling over $1 billion annually
- Smaller scale operations with profits of $30,000-$50,000 annually.

Personal Information Sales Earn Money

- Sale of personal information on just 50 credit or debit cards can generate earnings of $250,000-$1 million.
- Content theft websites make close to $227 million in ad revenue alone with overall revenues of around $4.4 million annually.

"The cost to acquire social security information, date of birth, residential addresses: $3."

Greater Effort Nets Greater Rewards

- Before being taken down in 2016, the Kickass Torrents platform was worth over $54 million, with estimated annual revenues of $12.5-$22.3 million in ad revenue alone.
- Individual criminals are now making up to £370,000 ($521,000) annually selling streaming devices that provide access to a wealth of film, television and other content.
- Many stores on the dark web have been found selling Remote Desktop Protocol passwords and other access credentials that provide access to thousands of Windows computers for $3-$100.

Platform Capitalism Looks Legit

Cybercriminals are taking a platform capitalism approach to selling, rather than committing, crime. These sites also offer customer reviews, technical support, descriptions, ratings and information on success rates. Some examples include:

- A zero-day Adobe exploit can cost $30,000.
- A zero-day iOS exploit can cost up to $250,000.
- Malware exploit kits cost $200-$600 per exploit.
- Blackhole exploit kits cost $700 for a month's leasing, or $1,500 for a year.
- Custom spyware costs $200.

- One month of SMS spoofing costs $20.
- A hacker-for-hire costs around $200 for a small hack.

What Cybercriminals Are Earning

- Individual hackers may earn around $30,000 for one or several jobs; but platform managers offering multiple card data forums can earn up to $2 million.
- Individual earnings from cybercrime are now, on average, 10-15% higher than most traditional crimes.
- High-earning cybercriminals can make $166,000+ per month.
- Middle-earners can make $75,000+ per month.
- Low-earners can make $3,500+ per month.

How the Money is Laundered

- 10% of the estimated $1.6-$2 trillion of laundered money in circulation can be attributed to cybercrime – totalling up to $200 billion.
- At least 30% of the sample of cybercriminals questioned as part of The Web of Profit research said they had physically transferred cyber revenues or sent money via couriers on airlines to deposit in foreign banks.

"95% of money mule activity has links to cybercrime activities."

- Digital payment systems were used as laundering tools in at least 20% of the cases sampled for this study – with PayPal playing some part in at least 10% of cases.
- 25% of bitcoin transactions are put through mixers.
- 95% of ransomware profits were cashed or laundered with the cryptocurrency trading platform BTC-e, which ceased trading after interventions from international law enforcement.

How the Money Being Stored or Saved

- 11% is in banks or building societies.
- 8% is in some other financial assets.
- 1% is in the form of vehicles.
- 1-2% of property transactions are directly funded by criminal activity – this equates to roughly 150,000-300,000 properties each year, worth around $3.7-$7.4 billion.
- 30% of cybercriminals surveyed reported attempting to convert revenues into hard cash.

"69% of criminal assets are stored in some form of property."

How Cybercriminals Spend Their Money

- 4% of laundered money is held in cryptocurrency – roughly $80 billion per year – even though 60% of cryptocurrency transactions can be linked to individuals.

How Many	What They Bought
15%	Used money to cover immediate needs
20%	Went to disorganised or hedonistic spending
15%	Spent on status items to impress girlfriends, other criminals, etc.
30%	Converted money to assets like property
20%	Some portion spent on reinvestments in further criminal activities

How Money is Being Reinvested

Around 35% of organised crime groups in the EU alone were directly involved in the production or trafficking of illegal drugs and 57% of dark web activity is now associated with trading in drugs.

British-born Al Qaeda follower, Younis Tsouli, provided technical assistance to the group and succeeded in gathering 37,000 credit and debit card data files, generating more than $3.5 million in revenues – money that was then reinvested into terrorist activity.

Chapter 1: The Web of Profit

Criminal practice has remained constant through the ages. There are standard ways in which our personal safety and our personal property are threatened – whether this involves assault or a burglary – and these have not changed much in substance since the earliest societies.

Many thought that the emergence of computer-related offending, or cybercrime as its accepted name now is, changed all this. And it is certainly clear that using malware or DDoS attacks to destabilise computers, or computer networks, appears to be a very different kind of criminal *method* than gaining entry to a target using – say – a hacksaw. But, in general, cybercrime usually involves the commission of familiar crimes, albeit multiplied and enhanced using computer networks.

The Cybercrime Economy and the Emergence of Platform Criminality

One of the headline findings that has emerged from this research involves the preliminary indicators of what may be a significant reconfiguration in the nature of criminality. In The Web of Profit, the old adage that crime doesn't pay may need to

be re-evaluated. We all know, of course, that crime very often *does* pay, but a fundamental recalibration of the relations between crime and its rewards now appears to be underway. In The Web of Profit, direct acts of crime often appear to pay *less* than the growing range of support infrastructures around them.

"What is especially fascinating about this phenomenon is how it appears to be mirroring shifts in the contemporary global economy."

Digital technology is now at the heart of a kind of post-crime reality, one where the most prolific criminogenic trends are less to do with the raw materials of crime – i.e. specific acts of criminality – and far more to do with how such acts can be mined, exchanged, and have secondary values extracted from them.

What is especially fascinating about this phenomenon is the way that it appears to be mirroring shifts within the contemporary global economy; shifts towards what has been called platform capitalism (Srnicek, 2016). This centres on the observation that platforms are now amongst the most powerful cultural and economic forces in society – companies like Facebook, Google, Amazon, YouTube, or the second wave, second tier platforms like LinkedIn, Twitter, Uber, WhatsApp, Airbnb, Instagram, Twitter or even Pinterest.

The main contribution of platforms is to connect the previously unconnected and allow individuals to share information in ways that (ostensibly) benefit them. For example, Uber and Airbnb let people connect directly to drivers or homeowners who wish to offer taxi or holiday rental services

without a middle man. Similarly, Facebook allows us to connect to old or new friends; YouTube allows us to share funny cat videos; and LinkedIn to link prospective employees and employers. The platforms themselves produce nothing in this process, whilst the users provide the platforms with the most precious of all commodities within an information economy – their data.

Today, data is a raw material that can be extracted, mined, sold and fashioned into new products and for new ends. The recent discovery that millions of Facebook user records had been illegally acquired and used by the U.K. data company Cambridge Analytica to influence the outcome of the 2016 U.S. presidential election (Lewis & Hilder, 2018) is a striking example of the increasingly common ways in which data acquired by platforms can now be subverted to further criminal purposes.

It is also becoming apparent that within the burgeoning cybercrime economy there are structures emerging that are very close to platforms; structures that are beginning to offer more attractive revenue-generating options. In this system, direct acts of crime become ancillary, playing a secondary role to the more important business of sharing criminal achievements and utilising the resources and services around them as revenue generators.

There seem to be at least two ways in which this emerging form of platform criminality is beginning to manifest itself within the cybercrime economy:

- In the use of existing platforms as sponsors for crime.
- In the development of cybercrime-specific platforms.

Weaponising Existing Platforms

The range of ways in which many of our leading and most respectable online platforms are now implicated in enabling or supporting crime (albeit unwittingly, in most cases) is astonishing and represents a significantly under-researched area of cyber-criminality. Data-gathering and field research for The Web of Profit project suggested at least four ways in which this is occurring:

- **Sources for Data Theft and Hacks**

  Given that data is the key raw material for platforms, it is not surprising that the data they acquire has also attracted the attention of cybercriminals. The 2013 to 2016 Yahoo! platform breach is considered to be the largest recorded to date and may have impacted up to 3 billion users (Perlroth, 2016). But there are many, many more.

  In 2013, Facebook admitted that it had exposed the records of up to 6 million users following a breach that went undetected for nearly a year (Shih, 2013). In 2014, Snapchat had user names and phone numbers for over 4 million of its users downloaded by hackers (BBC, 2014). In 2017, the We Heart It photo sharing platform confessed to a breach that had comprised over 8 million users' personal data (Perez, 2017).

- **Malware Distribution**

  With sizeable user bases, platforms also offer fertile ground for the distribution of malware, which often has multifaceted and varied purposes.

In early 2018, it emerged that cybercriminals had been abusing Google's DoubleClick network for a crypto-jacking attack – where malware runs the bitcoin mining software Coinhive on a victim's computer (Matthews, 2018). Elsewhere, in 2013, it was found that malware directed at the Instagram platform could artificially create likes in order to boost product profiles around brands (for a fee) (Vincent, 2013).

A completely different approach has been taken by cyber criminals who have exploited the LinkedIn platform by creating (very convincing) fake accounts as executives, vendors and the like to snare members into giving up personal details (Krehel, 2016).

With these in hand, phishing campaigns can be launched to download malware onto targeted corporate systems. Even better, the details of CEOs or executives can be illicitly acquired. Malware of this kind allowed the Carbanak cybercrime group to steal over $1 billion from more than 100 financial institutions (Reuters, 2015).

- **Illicit Supplies and Sales**

  During the course of this research it became evident how often platforms were being used to distribute or sell illicit or illegal products. It is not known how many counterfeit or illicit goods are now sold through Amazon and eBay, but most law enforcement agencies assume that the volume is significant.

  What is better known is the way these platforms are used to evade import duties or VAT. Undercover researchers found that the U.K. alone loses up to £1 billion a year in this way

and of course other sellers find their products are seriously undercut in price, forcing many out of business (Bowers, 2016).

Elsewhere, it has recently emerged that platforms like Twitter, Instagram and Facebook are being used extensively by drug dealers who often post with blatantly-obvious account names, such as 'ihavedrugs' (Ward & Mainment, 2017). Contacts are made, photos shared and negotiations then conducted over encrypted messaging platforms like Wickr.

- **Laundering**

  Since moving revenues around is a perennial concern for cybercriminals, the availability of commercial platforms where this can be done in plain sight has been a striking, if not predictable, development. Posts on Russian hacker forums have indicated schemes where legitimate or hacked Airbnb accounts are used to make bookings and payments to an Airbnb host who is collaborating with the scheme. Some of the profits can then be sent on and laundered, with no one ever actually staying in the property (Cox, 2017).

  In France, the government has complained that prepaid Payoneer cards, which Airbnb allows as a cashless form of property rental, are being used to launder money through Airbnb properties. The company has now bowed to pressure and will no longer accept them for payment in France (Vidalon, 2017). What Airbnb is doing with Payoneer cards elsewhere is unclear. Authorities in New York have become so concerned with the problem that they sent a letter to Airbnb, warning it to remove illegal listings on its site that could be used as a laundering resource.

In a more elaborate version of this kind of scam, it has emerged that one of the indictments against Paul Manafort, the chairman of Trump's 2016 presidential campaign, involved money he laundered that was used to purchase a $2.8 million apartment in Manhattan; which he then used to generate further revenues by renting it through Airbnb (Berson, 2017).

Another alternative is the use of platforms like Uber to launder money via accounts. In one scam, two accounts are created, with fake IDs. Rideshares (which never occur) are then paid for and money moved from an illicit revenue source like a stolen card to another kind of financial instrument (Teicher, 2018).

- **General Criminal Enablement**

  No one has yet done any detailed analysis on how platforms further crime in more general ways – for example, by putting criminals in touch with victims, enabling communication and conspiracy, jihadi recruitment and propaganda, and so on. Given the likely volume of crimes partly or more substantially enabled in this way, the volume is probably significant. However, without more research, the true level of criminal enablement provided by contemporary platforms is likely to remain an unknown factor.

Cybercrime-specific Platforms

The second variety of platform criminality – where platforms directly linked to cybercrime are used to generate revenues – is still a relatively new phenomenon. There are no

detailed studies of the trends, as yet. However, there are indications of at least three key variations on this theme:

- **Data Trading Platforms**

  Perhaps most obvious here are the many open web and dark web sites where platforms have been developed for the trade in stolen data. There are no figures for how many of these are in operation and any study of this kind would likely be out of date as soon as it was completed, given the speed at which these come and go – however, anecdotal evidence suggests that these may number in the thousands.

  The range of data types that can be purchased is extremely comprehensive. Aside from more obvious data materials, such as stolen credit and debit card details, it is possible to acquire social security information, dates of birth, and residential addresses across many nations, as well as other kinds of background information, often for no more than around $3 per record. Credit reports can also be purchased – with reports with a higher score (and therefore more useful for fraud) being sold at a premium rate.

- **Cybercrime-as-a-Service (CaaS) Platforms**

  A second, very well evidenced example of the nascent platform criminality model is crimeware or Cybercrime-as-a-Service sites. The range of materials and services available on such sites is almost overwhelming.

  Aside from specific tools, such as banking Trojans, one can buy or rent targeted DDoS attacks (by the minute, hour, day etc.); botnet infrastructures; known exploits (i.e. security holes in systems that allow penetration); hackers who can perform specific hacks on call; off-the-shelf duplicate or

new phishing websites; encryption services; and much more. There have even been apocryphal tales of criminal call centres available for rent (Johnson, 2017), which have a surprisingly wide range of applications.

In a phishing email campaign, victims are tricked into calling a number (such as banking support or tax inquiries) where their details are then harvested. CaaS sites often charge a kind of entrance fee for traders to join the site. The site owners can then simply sit back and let revenues mount up without doing anything other than providing a platform for trading to occur. With some observers claiming that fees of up to $100,000 have been charged for some sites (McKeon, 2017), the potential for such platforms to generate significant revenues is clearly evident.

- **BitTorrent and Download Platforms**

  These sites are well-known for supplying and hosting torrents around copyrighted work, such as film, music or software. Platforms such as Pirate Bay have been the target of numerous closure attempts by law enforcement and by the content-producing companies themselves. However, Pirate Bay has evaded all attempts to close it down and is still going strong. Together with a range of similar platforms – such as Rarbg.to, YTS.ag or Torrentz2.eu – a range of highly-profitable platforms are now in operation.

  What has been less well appreciated is just how the revenue model works. In a classic instance of platform criminality, the sale of advertisements and advertising space, rather than the sharing of pirated material, is where the profits are being made. For example, before its takedown in 2016, the KickassTorrents platform was worth over $54 million, with

estimated annual ad revenues of $12.5-$22.3 million (Fossbytes, 2017). Larger sites, like Pirate Bay, generate annual earnings in excess of $6 million; but even relatively small operators can command display advertising estimated to be worth around $100,000 per year.

These represent just a few examples of the most obvious, well-known sharing cybercrime economy sites that exist at present. Given the success of the platform model in both the legitimate and cybercrime economies it would be surprising if criminal innovation didn't expand and further develop this model in as yet unpredictable ways. What is clear, is just how much more lucrative these sites are for those who manage or run them, than for many of the individuals who contribute the data, or who do the grafting to obtain it.

In one recent example, an individual who ran and hosted a ransomware operation took two thirds of the profits for himself (Szoldra, 2016). Similarly, whilst it has been estimated that individual hackers may earn only $30,000 for one or several jobs (Brown, 2016), by offering multiple card data forums, academic research has suggested that managers can earn up to $2 million in some cases – often with just 50 stolen card details at their disposal (Holt et al, 2016).

Chapter 2:
Revenues from Cybercrime

Despite the obvious role of revenue generation as a primary motivation for engaging in cybercrime, it is surprising how little attention has been paid to its specifics. One possible reason for this has been the greater attention paid to one of the most commonly recycled cybercrime metrics – estimates of the costs and losses it entails.

"Estimated global revenues from cybercrime: $1.5 trillion+ annually."

Trying to determine cost has been something of an obsession amongst both researchers and policy makers and (as the table below indicates) there continue to be attempts to update earlier estimates; such as the £3 billion cost to the U.K. per year, provided by Detica (2011).

However, there have been a number of confusions around the use of cost metrics, which have somewhat muddied the water. Is the cost of cybercrime always the same thing as losses

from cybercrime, for example? A major confusion has been the assumption that, in arriving at an estimate of costs – however precarious – we also acquire an estimate of *revenues*. For example, Norton (2011) made an equation between the global *cost* of cybercrime with *profits* made from trafficking in marijuana, heroin and cocaine. Such claims often depend upon recorded losses, rather than genuine revenues.

Estimated Annual Costs of Cybercrime	Source
Globally: $6 trillion by 2019	Cybersecurity Ventures, 2017
Globally: $799 billion to $22.5 trillion	Dreyer et al, 2018
Globally: $400 billion+	CSIS, 2014

Table 2: Cybercrime Cost Estimates

It should be clear that losses from cybercrime cannot be assumed to directly translate into the revenues or profits that accrue to cybercriminals as a result of their offending. For example, included in any figure for losses will be factors such as costs of policing and security, or repairing any damage that has been done. Put simply, a cybercriminal cannot *spend* the costs of extra cybersecurity.

> "Over 50% of cybercrime revenues are generated through online markets."

There are, of course, numerous caveats that must inevitably accompany any estimate of cybercrime revenues. One of the most obvious difficulties involves the ongoing debates about

what to *include* as a cybercrime – decisions made here can radically affect any estimated total. Take, for example, counterfeit goods: the great majority are now sold via online markets. Trade in such goods provides one of the highest cybercrime revenue generators (see below), so if it were decided that they should not be included, removing them would significantly alter any evaluation of cybercriminal profits.

This problem is a reflection of wider debates in the field about the nature of cybercrime, in particular how far *cyber-enabled* crimes (i.e. crime not dependent upon a computer, malware distribution) count as cybercrime. Enablement is a notoriously vague concept in causal terms – do indirect actions like drinking a cup of coffee before committing a crime enable it in ways similar to the use of more direct and obvious tools? For the purposes of this report, **cybercrime revenues are identified as any revenues arising from crimes where computers play an obviously direct role.**

A second and equally crucial difficulty for arriving at credible estimates of revenues relates to the problems in obtaining reliable or sufficiently comprehensive data. Criminals do not readily provide details of how, or in what way, they acquire revenues. Similarly, law enforcement, private business and security professionals are invariably cautious about revealing information that might affect sensitive operations.

"A third of cybercrime revenues are linked to theft of abstract commodities like corporate secrets and other IP."

Of course, this is a problem for cybercrime research in general – even where it involves ostensibly transparent sources, such as court and police records. For example, such records tell us nothing about revenues and even where assets have been seized, there is rarely a lot of clarity about how they were used.

But nor does the scarcity of data mean that it is *impossible* to arrive at some conclusions about revenues, albeit highly provisional ones. Small samples in social research can warrant general inferences, just as triangulating across multiple sources can help refine and focus otherwise unclear patterns in the data.

"Cyber-criminality now offers a portfolio of activities where profits can be substantial and relatively easy to obtain."

For this research, the above estimate was obtained by utilising five revenue-generating cybercrime activities – activities that are both prominent and relatively well-evidenced. By extracting indicators from a variety of primary and secondary sources, revenue metrics were then developed for each of the selected area of cybercriminal activity and these were then totalled to arrive at an initial estimate for the current global revenues being generated by cybercriminals.

For this report, the five areas selected and their estimated revenues were[1]:

[1] Details of these estimates are contained in the methodology section of this report

Crime	Annual Revenues
Illicit, illegal online markets	$860 billion
Trade secret, IP theft	$500 billion
Data trading*	$160 billion
Crimeware, CaaS	$1.6 billion
Ransomware**	$1 billion

*Revenues derived from trading in stolen data, such as: credit and debit card information banking log-in details, loyalty schemes and so on
**Revenues derived from extortions based on encrypting data and demanding payments

Table 3: Annual Cybercrime Revenue Estimates

These estimates confirm what many have suspected – that cyber-criminality now offers a portfolio of activities where profits can be substantial and relatively easy to obtain, compared to traditional revenue-generating criminal activities, such as armed robbery, burglary or street crime.

There is a slight artificiality to the chosen categories – for example, as mentioned previously, ransomware could be included as a type of crimeware. But given that it has become a very high profile and well evidenced form of revenue generation in a short time, it was decided to treat it separately. In future work of this kind, it is hoped that revenue categories and the estimates associated with them can be refined and further developed.

As with any estimate, there is an element of art as well as science in deriving it, but it is important to be clear that this is a *highly conservative* estimate – the real figure is likely to be significantly higher.

There are several reasons for this:

- **Revenues Remain Invisible**

  The figure is derived from only the above five categories of cyber-criminality. Many other areas that generate revenues remain invisible or can only be incompletely captured in terms of numbers. For example, frauds using mass communications (like 419 or romance scams) were not included but would have boosted the above estimate.

  In the U.K., such frauds earned around £3.6 billion ($4.9 billion) in 2015 (CCFS, 2016), in the U.S. they earned approximately $25 billion (ICE, 2010) and in Australia, they earned around AU$94 million ($74 million) (Whitty, 2015); thereby generating an estimated total of over $29 billion. But because of difficulties in obtaining reliable global data for this and because it doesn't appreciably alter the working $1.5 trillion estimate above, the category was omitted for this report.

- **Estimates Likely Under-Represent**

  Even within the categories listed, associated estimates are likely to under-represent, rather than over-represent, the real amounts being generated. For example, within the crimeware category, revenues were only counted for three types of activity: DDoS and botnet hire, sales of Trojan-related malware, and hacker-for-hire prices. Similarly, the figure for revenues from illicit/illegal online market sales was based only upon sales of three kinds of commodity: illegal drugs, illicit or illegal pharmaceuticals, and counterfeit goods. There are many other examples of revenue generation that could have been considered within each of the specified revenue categories, but since evidence was poor, or inconsistent, these were omitted.

- **Conservative Estimates Balance the Cost**

  In most cases the lower, more conservative end of a revenue range was selected, where an estimate range was available. This was to provide one way of accounting for the *costs* of the relevant criminal enterprises. This is a somewhat arbitrary approach, but since other attempts to estimate the costs of engaging in cybercrime have not been convincing (Anderson et al, 2012), it is probably as good as any other. Either way, without some provision for cost, it is only estimates of revenues (rather than profits), which are derived. Without some sense of profits, laundering and spending by cybercriminals cannot be estimated. In general, the term revenues, rather than profits, is used throughout this report; this is partly for simplicity and consistency, but also because revenues are generally a little easier to estimate than specific profits.

Given these qualifications, it is highly likely that future researchers who look at cybercrime revenues will arrive at higher totals than what has been suggested here. But, on the rationale that it is better to use only what we can be reasonably sure of, these totals can at least form a starting point for such research.

Cybercrime Revenues vs. Traditional Crime Revenues

Cybercrime is often now argued to be more significant than traditional crime. The most common rationale offered for this claim is the perception of explosive growth and year-on-year rises across all its categories. Less common has been any

attempt to evaluate their relative significance by comparing the different revenues they generate.

Understanding of traditional criminal revenues is better developed than is the case with cybercrime – not only are there more data sources available, there has also been a lot more experience in measuring profits and losses from traditional crime. For this reason, it is useful to begin by looking at what we know about revenues from traditional crimes.

"Cybercrime is often now argued to be more significant than traditional crime."

Previous research conducted by the U.K. Home Office (Dubourg & Prichard, 2008) on profits from organised crime in the U.K. offers one set of precedents for evaluating comparative revenue levels within cybercrime. Comparisons are most evident in the level of profits generated by drug sales and drug trafficking and in the significance of fraud as the other highest revenue-generating category.

Sector	Annual Profits
Drugs	£5.3 billion
Excise Fraud	£2.9 billion
Fraud	£1.9 billion
Non-excise IP Theft	£840 million
People Trafficking	£275 million
People Smuggling	£250 million

Table 4: U.K. Organised Crime Profits in 2008

A more recent global study (GFI, 2017) looked more specifically at transnational crime and offered the following range of estimated annual profit values from crime (see table below).

A first observation is that the cumulative total of revenues ($1.6-$2.2 trillion) for this measure of traditional crime only exceeds that for cybercrime at the upper range of the estimate (i.e. $2.2 trillion, as opposed to $1.5 trillion). Given that cybercrime is a relatively new criminal phenomenon, with methods that are relatively new and evolving, this comparison offers a more immediate and tangible reason for treating it as seriously as traditional offending.

Transnational Crime	Annual Profits
Counterfeiting	$923 billion–$1.13 trillion
Drug Trafficking	$426-$652 billion
Human Trafficking	$150 billion
Illegal Logging	$52-$157 billion
Illegal Mining	$12-$48 billion
IUU Fishing	$15.5-$16.4 billion
Illegal Wildlife Trade	$5-$23 billion
Crude Oil Theft	$5.2-$11.9 billion
Illegal Firearms Trafficking	$1.7-$3.5 billion
Organ Trafficking	$840 million–$1.7 billion
Trafficking in Cultural Property	$1.2-$1.6 billion
TOTAL	**$1.6-$2.2 trillion**

Table 5: Estimated Global Profits from Transnational Crime

It is also worth remembering – as this report suggests – just how far many traditional categories of crime are now interdependent with cybercrime. For example, how far does digital technology help further the $426-$652 billion made from drug trafficking, or the $923 billion to $1.13 trillion generated by counterfeiting? If – as the suspicion must be – many of these traditional activities have elements that are dependent upon the digital, then it is likely that many traditional crime activities of the kind listed above are already cyber-enabled in some sense and so could also be counted under revenues from cybercrime.

Individual Revenues from Cybercrime

Estimates of the profits from crime – traditional or otherwise – tend to relate only to measures at a very general level. They do not, in other words, tell us very much about how such revenues are *divided-up* amongst criminals, or the kinds of revenues which accrue to individuals involved in criminal enterprises.

"Individual earnings from cybercrime are now on average 10-15% higher than what can be earned from most traditional crimes."

Since distribution is presumably unequal, some perpetrators will acquire more revenue for disposal than others and this has obvious implications for the ways in which criminals spend their money. Organised crime group (OCG) leaders, for example, will likely be more aware of the need to reinvest, or to divert funds to support further criminal activities.

By contrast, foot soldiers will have fewer constraints. As such, they will be more likely to engage in impulse or ostentatious patterns of spending. There has been limited research on the inequalities in the distribution of criminal revenues, or the revenues acquired by individual criminals in general. So, we are largely dependent upon a fairly small body of empirical studies conducted in the 1980s. As a result, our understanding of the likely contemporary earnings by individual criminals lags a little behind the facts on the grounds.

One study, (Freeman and Holzer, 1986) drew upon a sample, of 2,358 minority youths in Boston, Chicago and Philadelphia, that was obtained from the NBER Survey of Inner City Black Youth, conducted in 1979-1980. Using this data, Viscusi (1986) estimated that income from crime stood at around $1,504 annually – relatively high given that legal earnings within the same sample stood at around $2,800. It is significant that, even when filtered down to individuals, there are some obvious and ongoing continuities in high revenue-generating activities within traditional crime and revenue-generating activities for cybercriminals. For example, Viscusi's research indicated that drug-dealing earned about one-third more than property crimes for individual criminals.

This pattern has also been seen in more recent research on criminal earnings, such as Nguyen and Loughran's (2017) study, which compared data on (self-reported) illegal earnings collected within two independent surveys. Their research was able to filter revenues against a range of project costs, expenses and other factors ("inflated outliers"). Their findings continue to mirror previous work in this area, indicating that we can have some confidence about identifying high-yield revenues and their continued attractiveness to cybercriminals.

"Assessing profits for individual cybercriminals is even more complex given the scarcity of data."

The Nguyen and Loughran study found that street dealing and selling drugs produced an average weekly income of $900. Earnings were comparable to other traditional low-level criminality, such as robbery, burglary, and check forging, though such activities are usually more involved and higher risk than drug dealing.

These income levels were also corroborated in work by Bouchard and Wilkins (2008) which found (mostly organised) criminals with median annual income of around $46,000 – that is around $884 per week – very close to the Nguyen and Loughran figure.

Assessing profits for individual cybercriminals is even more complex given the scarcity of data and the obvious difficulties in assembling large enough samples to produce credible income averages. Nonetheless, some limited inferences can be made based upon what we do know about the profits made by convicted or active cybercriminals in certain cases. For example, in a sample of six recent arrests of large operators, confiscations of between $1.5-$2.5 million in Bitcoin or other forms were made. On the assumption that this approximated yearly revenues from their operations, it works out at around $166,000 per calendar month, based on the midpoint of the scale.

This compares fairly closely to traditional crime – with the important caveat that there are now far more individuals able to acquire such revenues through cybercrime than was previously the case. At the middle-income range, cybercriminals in our

sample earned on average between $50,000-$100,000 annually (for an operation or operations roughly of this duration) resulting in a mid-point scale income of around $75,0000. Low incomes were calculated on the lowest reported incomes for a single operation and compared to incomes in the Nguyen and Loughran study that also ceased after 1-2 operations (for example, because a street criminal was caught, or desisted from further activity).

This gives us the following comparative estimate of the earnings of traditional criminals versus cybercriminals:

Criminal Rank (earnings per month)	Traditional Criminals	Cyber Criminals
High Earning	$130,000+	$166,000+
Middle Earning	$40,000+	$75,000+
Low Earning	$1,800+	$3,500+

Table 6: Traditional vs. Cybercriminal Annual Earnings

These figures obviously have a speculative aspect without a larger sample to draw upon, but together with other available evidence, certain indicative patterns seem to emerge:

- In general, the very spectacular earnings made by high-profile traditional criminals, especially organised crime group leaders of the kind detailed below, still tend to outstrip very high earning cybercriminals.
- However, earnings made by cybercriminals at a less spectacular high-and-middle range often match or outstrip those from traditional crime. For example, research by Holt et al (2016) around a high-end, lucrative operation suggested that the sale of personal information on just 50 cards could

generate potential earnings of around $250,000-$1 million. By contrast, the activities of many online drug dealers indicate a kind of middle income bracket. Data obtained for this project suggested that online marijuana or cocaine sales could net between £60,000-£80,000 per annum (over $112,000), while steroid sales could net up to £100,000 (about $140,000).

- If a lower level income bracket is construed in terms of relatively modest one-off operations of the kind suggested above, then cybercrime operations appear to produce better revenues than one-off street criminal operations, with far less work and (usually) far less risk.

"There is some evidence that hackers and other front-line cybercriminals often do the hard work, but benefit far less from it."

In a sign of the developing platform crime model there is some evidence that hackers and other front-line cybercriminals often do the hard work, but benefit far less from it than those who run the platforms where their data is sold. One study (cf. Szoldra, 2016) examined an organised Russian ransomware group and was able to establish that, on the basis of 30 ransom payments received at $300 each, around $7,500 was going to the leader of the group – a substantial cut.

As suggested, very spectacular levels of earnings have been excluded from the estimates in this section, given that these are likely to be exceptions to the norm. For example, traditional criminals like the Mexican drug dealer Joaquín Loera (El Chapo) – who was listed as the 937th richest man in the world by *Forbes*

in 2010 (with personal assets of at least $1 billion). Or Yakuza Godfather, Susumu Ishii, who made over $1.5 billion through loans, banking deals and real estate scams. Or Amado Carrillo Fuentes, who made around $25 billion through cocaine sales. We know less about the very spectacular earners from cybercrime, but Ross Ulbricht of Silk Road reputedly accumulated a personal fortune of up to $1 billion.

Chapter 3: Key Revenue Sources for Cybercriminals

If profit is now key to understanding what drives cybercriminality and its infrastructures, then a more sophisticated awareness of the key revenue sources for cybercriminals is essential. Whilst we have some knowledge of specific types of revenue generation this tends to be rather fragmented and lacking in the kind of integrated overview that can provide the strategic advantages to enable more informed varieties of intervention and disruption.

In this section, some of the more prominent means by which cybercriminals profit from their activities are reviewed and the relative incomes they can generate evaluated. It is important to be clear however, that what follows is only a selection. The Web of Profit is likely to be far more complex and far more lucrative than what this research has been able to detect.

Revenues from Illicit Online Markets

Amongst the many paradigm shifting impacts of the internet, one of the most promising avenues of opportunity for cybercrime has come from the development of ecommerce and the buying and selling of goods via online marketplaces. In 2017 alone ecommerce sales increased by 23.2%, accounting for one-tenth of total retail sales. The total *value* of these sales is now close to $22.737 trillion, up 5.8% from their value in 2016 (Chaffey, 2017). In Europe, 68% of individuals now say they regularly shop online (Eurostat, 2017).

"Illicit online marketplaces have minimum annual global revenues of $860 billion."

The growth of *illicit* marketplaces, which parallel legitimate ecommerce sites, has been a striking development that makes a substantial contribution to The Web of Profit and which offers one of the most telling indicators of the way it mirrors the legitimate economy. The result has been a revenue stream that is amongst the most significant of all – providing over 50% of total cybercrime revenues at present.

There are at least two variants in the use of online retailing to generate criminal profits:

- Revenues generated by the misuse of legitimate online markets – for example, via auction frauds and fake ads.
- Revenues generated by selling illegal or illicit goods in online markets.

The new proclivity for shopping or conducting business online presents a number of opportunities for exploitation. This

might involve advertising items that may not exist, or are of a far lesser quality than what is advertised. It may also involve fake websites where money or personal details are harvested.

There are two basic ways in which this can be done: copying or duplicating an original and authentic site, or creating one from scratch. Users can be directed to the fake site using techniques such as DNS spoofing and although duplicate sites can often be blocked by browsers such as Chrome or Safari, there is evidence that JavaScript can be used to block browser popups (Bengineer, 2015).

Numerous examples of fake ecommerce sites have been found in China and Japan, advertising hundreds of products for sale in different sizes and at different prices, with a range of different payment methods (Isaza, 2015). Others generate revenues by selling fake goods. Since 2015, U.K. police alone have closed down over a thousand websites selling fake luxury goods, such as Burberry, or Abercrombie & Fitch (BBC, 2015).

Other sites might offer rental properties that don't exist, or are already occupied, or tickets, holidays or similar leisure items that never arrive or that, again, do not exist. Even sites that sell relatively low-value items can still be profitable, if repeated enough times.

Whilst average losses (to a purchaser) from ticketing frauds run at around £80 in the U.K. (Button and Cross, 2017), nine individuals who were arrested in the U.K. in 2014 were found to have defrauded around 850 individuals by selling fake tickets to concerts such as Arctic Monkeys, Arcade Fire, Beyoncé and the Reading Music Festival. This ostensibly low-key operation had made up to £116,000 by the time the criminals were detained (Southport Local, 2014).

Though the criminal exploitation of legitimate marketplaces can be relatively easy and low cost to implement, the profits to be made from this kind of revenue stream are not easy to calculate. Major online retailers are not very forthcoming about how many transactions involve fraudulent buyers or sellers, though we know profits can be substantial. For example, just one couple made up to $1.2 million by manipulating Amazon's returns policy – in some cases receiving replacements even before the original goods had arrived (Steiner, 2017). However, we do know that the trade in counterfeit goods, which many such sites specialise in, can generate huge revenues – over $800 billion, according to reliable sources.

"Of all varieties of illegal goods sold online, it is probably the drug market that has attracted the most attention."

Investigating the world of illicit or illegal commerce on the dark web is far harder – not just because navigating it is less straightforward than the regular internet, but because many of the sites only grant access by word of mouth, or on the basis of ratings status and trust, which may take some time to build up.

Of all varieties of illegal goods sold online, it is probably the drug market that has attracted the most attention. In one recent study, *The Economist* looked at revenues being generated within three online markets selling illegal drugs, legal pharmaceuticals and firearms (Economist, 2016). It found the drug market to be the most profitable – around $27 million in sales between December 2013 and July 2015, with marijuana and MDMA sales constituting around 50% of this total.

Before its takedown by law enforcement, one of the largest dark web markets, AlphaBay, carried 68% of all drug listings, with 250,000 separate entries; 30% of which involved class A drugs (IOCTA, 2017). These estimates appear to be very conservative when compared to other revenues seen in other evidence sources. For example, following the takedown of the online drugs market Silk Road, prosecutors claimed that the operation made over $1.2 billion during the 2.5 years it was operational; with the site administrator, Ross Ulbricht, making around $80 million in commission. Ulbricht denied this, claiming most of these amounts had been put back into operations and growth. By 2013, the FBI had seized $34.5 million in Bitcoin accounts they claimed were linked to Ulbricht (Greenberg, 2013), with another $22 million in circulation that the FBI couldn't reach.

But recent research (Kruithof et al, 2016) appears to confirm that the online drug market is nowhere near as large as the global drug market as a whole – which in the U.S. alone, generates an estimated $100 billion per annum. The study estimated such sites make up to around $180 million per annum – indicating there is some way to go before it attains equivalent revenues, though this might not be long, given that sales volumes have tripled in recent years.

By contrast, the sale of illicit prescription pharmaceuticals online constitutes a significant slice of criminal income – around $400 billion in total.

IP and Trade Secret Theft

Generating revenues through the theft of ideas (Wall, 2016) is, like most cybercrimes, nothing new. Even in Ancient Greece,

sculptors were forced to put trademarks on their work to prevent others claiming the work as their own. But the advances in technology have impacted upon the opportunities for profit here considerably. For example, the Statute of Anne Copyright Laws (1710) in the U.K. created the first legislative framework around the right to copy and were a specific response to the new technologies of printing and the sudden spread of pirated books and pamphlets this had facilitated. Three hundred years later, digital technology offers the latest tool for enabling someone's ideas to be turned into revenue streams for others and has created a whole new income stream for criminals willing to profit from someone else's work.

"IP and trade secret theft has minimum annual global revenues of $500 billion."

The first wave of this centred on intellectual copyright, related to film, music and content downloading. This created a wave of moral panics about the potential damage to artists' rights – largely driven by the creative industry's wish to retain monopolies on their product. It also generated some fairly quick responses – from draconian public punishments of a few symbolic offenders, through to locked-down proprietor content, purveyed through sites like iTunes.

Permutations of this still offer reasonable revenue streams – for example, music piracy alone has been estimated to be worth around $12.5 billion per annum (Siwek, 2007). However, cybercriminals have evolved more ingenious ways of monetising stolen content, which now generate far more substantial income

streams – especially by way of platforms. Typically, these include:

- Selling ads on sites where illegal content can be acquired.
- Selling subscriptions to such sites.
- Selling copies of items like pirated software, or planting malware on such sites.

The creative ways in which IP can now be exploited to generate revenue is illustrated by the fact that content theft websites made $227 million in ad revenue alone in 2014 **(**DCA, 2014)**.** Sites that profit exclusively from advertising produce an average revenue stream of around $4.4 million annually, with the most heavily-trafficked BitTorrent and P2P portal sites topping $6 million annually. Even smaller sites studied here could make more than $100,000 a year in advertising revenue.

The platform criminality model can also be seen in the way that direct acts of stealing are gradually being augmented by intermediary sales methods. For example, rather than spending time acquiring illicitly copied content, some criminals are now making up to £370,000 ($521,000) per annum by selling the streaming devices that provide access to a wealth of film, television and other content (Sulleyman, 2017).

"Cyber espionage is rated as the most serious threat to their business by 20% of global organisations."

Estimates of revenues from copyright infringement in the U.S. alone have been put at around $300 billion (IPC, 2013) so the global figure is probably much higher. But a substantive part

of the total for IP theft revenues suggested above now comes from the theft and sale of corporate IP, corporate trade secrets and corporate data – for example, business plans, new product development and the like. There are many difficulties in establishing clear revenue totals here, given that many perpetrators are governments and other corporations whose gain is often more abstract than monetary, but even on modest assumptions this trade is likely to be worth around $200 billion per annum (see appendix for discussion). It is no surprise then, that recent research (Trend Micro, 2017) has suggested that cyber espionage is rated as the most serious threat to their business by 20% of global organisations. Around 20% of U.S. organisations have suffered a cyber espionage-related attack.

"Company staff appear to be using underground sites, such as the Kick Ass Marketplace or Stock Insiders, to sell trade and financial secrets."

There are good reasons for their concerns. One problem is the sheer cost – recent survey data suggests current estimates of the average cost of a data breach now stand at around $5 million; ranging from $13 to $217 per record (Ponemon, 2015). Other challenges are more technical; for example, the availability of new cyber espionage tools like Copperfield, which is based on the four-year-old remote access Trojan, H-Worm. The malware tool is likely designed for data theft and reconnaissance, but has also been implicated in attacks on critical infrastructures.

Another version of this problem is the constantly evolving tactics used by organised groups to install malware that can steal data on targeted corporate systems. For example, the Russian cyber espionage Turla gangs have recently been found to have disguised their malware by using a legitimate IP address, which appears to belong to Adobe Flash installer (Apps & Finkle, 2014). Their many victims have included the U.S. Department of State.

Elsewhere, evidence emerged in 2017 of the sale of remote access credentials to gain access to Windows computers using Microsoft's Remote Desktop Protocol (RDP). This allows individuals to access virtual desktops and permits the systems to be managed remotely by criminals, in order to steal corporate data. The trick is particularly effective in that it does not need malware to succeed and once in, cybercriminals have the luxury of accessing almost anything they want – usually without the victim's knowledge.

A variety of underground stores on the dark web have recently been found selling RDP passwords and other access credentials for $3-$100. Once purchased, data from thousands of Windows computers become available for theft. For example, dark web sites like Ultimate Anonymity Services or xDedic were found to be offering thousands of RDP credentials allowing access to Windows XP and Windows 10 computers in the U.S., China, Brazil and India (Palmer, 2017).

The trade in corporate secrets is also being significantly furthered by the increasing number of insiders implicated in trading in them. Company staff appear to be using underground sites, such as the Kick Ass Marketplace or Stock Insiders, to sell trade and financial secrets. The Kick Ass Marketplace (which appears to be different from the similarly named Torrent site,

though this is not clear) provides expert oversight on the data, rating it on a scale of accurate to bad and even provides advice on choosing stocks and investing. Known members of the site include investment firms, who appear to be seeking to gain competitive advantages by using it (Darknetmarkets, 2017).

By contrast, the Stock Insiders site appears to be more brazenly criminal and has even been found to be enticing bank staff to provide stolen credit card information. It has also been claimed that the site has been seeking to run operations involving the recruitment of individuals willing to pretend to be the owners of the stolen cards. In-store tests can then be run on whether the cards work. Evidence was also found of store workers being recruited to assist with these operations.

Companies with high value intellectual property, like pharmaceuticals, have been particularly hard hit by this kind of corporate theft and they now try to cooperate closely with law enforcement to infiltrate sites like Enigma. This open-web marketplace was focused purely on matching sellers of corporate information with prospective buyers, but has now ceased to operate because it suspected penetrations by investigators (Krebs, 2016).

The willingness of bankers to use such sites to gain advantages in the market by insider trading and other malfeasance, or of companies stealing sensitive information from others, is a striking instance of the way that The Web of Profit has been blurring the legitimate and the cybercrime economies. The profits made by such sites also further illustrates the attractions of the platform criminality model. The Kick Ass Marketplace site alone was estimated to be making over $30,000 every month from such activities and has a Bitcoin wallet of around 200 bitcoins (Darknetmarkets, 2017). Like

platforms in general, the owners of the sites can let others do the criminal work and simply make their money by providing a meeting place where this information can be shared.

Revenues from Data Trading

A far more established revenue generator within the cybercrime business model has been the technique of acquiring, or intercepting, personal data and then using it fraudulently. This does not just involve the misnomer of identity theft, but can involve just about any form of data that has convertible value.

The shift to electronic versions of our money – that is, the use of debit and credit card transactions as exchange mechanisms and the advent of online banking – has provided wholly new spaces of criminal opportunity. The acquisition and trading of this and other data types represents one of clearest contiguities between The Web of Profit and the legitimate economy, where data is now a prime commodity.

"Data trading has minimum annual global revenues of $160 billion."

This opportunity has been expertly exploited by cybercriminals and has produced two main revenue-generating variants:

- Revenues acquired through fraudulent use of data, such as personal information (that is, card or banking fraud).
- Revenues acquired through trading in data.

Figures from card and banking fraud offer one of the more reliable sources for measuring revenues from data theft. Not only are these figures comprehensively recorded by banking and card authorities, this is one context where losses can justifiably be read as revenues (since it is the criminal spending on the card that directly translates into its losses). Some caution is necessary, since many sources double-count the misuse of data. For example, sources like the annual U.K. Financial Fraud Action reports include figures for losses from card data used remotely within figures of losses from ecommerce. However, it is still possible to gain a reasonably accurate estimate of revenues from misused cards by combining the total losses from the U.S. and Europe.

In 2015, recorded losses from card fraud amounted to around $22 billion (Nilson, 2016), whilst in Europe there is a fairly robust estimate of losses provided by FICO of around $1.8 billion in 2016. The U.K. accounted for the largest proportion of losses, at around £600 million (FICO, 2016). Rounding up, this suggests that cybercrime revenues from the actual use of stolen cards alone comes to $24-$25 billion.

However, the use of stolen cards represents just one part of the revenues that arise from data. *Trading* in data also needs to be taken into account and may be providing revenues far in excess of actual use. The existence of numerous large platforms where data and many other commodities can be bought or sold is now well established and, prima facie, evaluating revenues made here is easier than assessing other kinds of cybercrime profits because of the transparency in pricing.

Large platforms like AlphaBay or The RealDeal may have been taken down in the last couple of years, but there are many more that have stepped in to replace them. Many of these sites

demonstrate the mark of the platform criminality model with links to Facebook and Twitter pages and are supported by news and information sites, like DeepDotWeb, which offers information and guidance for those wishing to access data trading sites.

Research by Holt et al (2016) on one such site (also called a carding forum) found that just 50 stolen cards could yield revenues of $250,000-$1 million for the individual or group that traded them.

Other indicators of revenue here can be seen in examples such as the recent takedown of the Infraud data-trading site, which acted as a kind of Amazon of cybercrime. This site offered the sale and purchase of stolen dates of birth, addresses, passwords, social security numbers, payment card details and other personally identifying information, amongst an impressive portfolio of wares. The operation was estimated to be worth around half a billion dollars when it was taken down.

But in spite of the relative transparency of information about revenues, calculating any kind of plausible total here is far from straightforward. One obvious problem is the volatility of pricing. Supply and demand issues play a big part in this, with scarce data commanding far higher prices than more easily available examples. For example, the huge breach of the Target chain that occurred in 2013 was estimated to have very quickly caused a fall in prices from $15-$20 per card record to $0.75 per card record. There is also, of course, a lack of certainty around how much data is actually sold across such sites.

However, we know that around four billion data records of different kinds were stolen in 2016 (RBS, 2016). By then taking just three kinds of data traded across sites (credit and debit card data; banking or payment system data; and login data to

resources such as Netflix or app accounts) and averaging the price of these across various sites, it was possible to arrive at an estimate of around $160 billion in annual revenues currently generated by data trading. If other data traded across sites – for instance, loyalty points, credit files, medical records, or social security details – could also be costed and included, this total would presumably be far higher.

Revenues from Crimeware & CaaS

At the core of the emerging cybercrime economy and its platform approach to generating revenues are the increasing range of services that offer support for the commission of cybercrimes. This form of revenue generation is not the most lucrative. But the revenue stream is a fairly new one and given its rapid rate of growth, there is presumably more to come.

"Crimeware and Cybercrime-as-a-Service has minimum annual global revenues of $1.6 billion."

The development of an income stream around the selling of tools and services for committing cybercrime is a telling illustration of how serious cyber-criminality has come to depend less upon the commission of specific crime itself and more upon the platform capitalism approach of selling, rather than committing, crime.

In essence, the crimeware revenue stream is a service industry, which may have origins in providing the tools for cyberattacks, but which has now evolved into a kind of off the peg warehousing facility, where whatever is needed for the

commission of cybercrime can be bought or hired. Thus, instead of the traditional, romanticised image of the techno-savvy hacker, criminals who make their profits in this way tend to have more in common with retailers or service providers – providing add-ons like technical support or customer feedback.

Estimating the kinds of revenues that can be generated here involves one of the complex calculations of this kind. There is certainly evidence available if one can gain access to sites where such materials are on sale. But several factors make the task of arriving at definitive revenues very hard:

- The sheer number of such sites now accessible.
- The rapidly changing prices.
- The different kinds of prices that can be charged for different kinds of crimeware.

For example, in 2012, on sites looked at for this research, a zero-day exploit for Adobe might cost anything from $5,000-$30,000; whereas a similar tool for iOS might cost up to $250,000 (cf. Ablon et al, 2014). Similarly, a malware exploit kit could have been obtained for as little as $20 in 2006, whereas the minimum now tends to be around $200.

As with any retailing enterprise, some products will be more popular with consumers than others. For example, Blackhole, one of the most successful exploit kits, was (at its height) for sale for $700 for a month's leasing, with a year-long license costing $1,500 (Krebs, 2013).

The shopping list characteristic of many crimeware sites, mean there is often a range of pricing options for malware or exploits which are offered. One example from a Russian website, offered products for anything between $200-$600 per

exploit. These exploit weaknesses in the Opera system, providing helpful descriptions, ratings for success and, of course, cost.

"Custom spyware could be created for around $200, or a month of SMS spoofing hired for only $20 per month."

There are plenty of more economical options available too. For example, a study that compared prices listed for various services from five leading crimeware providers on the dark web (cf. Barth, 2016) found that custom spyware could be created for around $200, or a month of SMS spoofing hired for only $20 per month. And in addition to tools, it was also possible to hire specific trade skill. Much like hiring electricians or plumbers on sites like Checkatrade, sites like Rent a Hacker provide hacking services, with an average cost for a small hack around $200.

By focusing on just three kinds of services – DDoS or botnet hire; malware purchase or hire; and the rental of hacking services – and finding average costs of these across five platforms where such services were on offer, it was possible to determine the above estimate of around $1.6 billion in annual revenues. Again, this is likely to be significantly lower than what is actually earned, given that there are usually many more services on offer on such sites. Amongst the many un-costed examples found during this research were: cloud-based DDoS attacks; access to Gmail; manipulation of ratings on sites like TripAdvisor; changing essay grades; deleting records (e.g.

licence points or criminal records); or even enhancing Amazon and other product reviews.

Revenues from Ransomware

Placing (or threatening to place) encryption malware on systems unless payments or ransoms are paid is perceived as a relatively new crime phenomenon, with the rise to current levels beginning about six years ago (around 2012). Of course, generating revenues via threat or extortion is a long-established criminal practice and has earlier precedents within cybercrime.

For example, Grabosky reports how in 1993-1995, £42 million was extorted from institutions by being told their systems had crashed (Grabosky et al, 2002). But the origins of ransomware proper begins from around 2008, when the use of Scareware – software that sent real or frivolous threats about dangers to a device or a system – began to be noticed more widely.

"Ransomware has minimum annual global revenues of $1 billion."

In terms of revenue generation, however, these antecedents to ransomware were relatively unsuccessful. As cybercriminals have refined the ransomware model, the spike in earnings has been dramatic. For example, the Cryptowall ransomware, which emerged in 2014, has been estimated to have generated anything from $18-$320 million in profits. Its success led to over 100 variants in the 2014-2016 period and helped create the impression that ransomware now represents the most profitable cybercrime.

In a recent study by researchers from NYU and UC San Diego (in partnership with Google) it was reported that victims of ransomware had paid out around $25 million in ransoms over the last two years (UCSD, 2017). This amounted to an average of over $1 million per month.

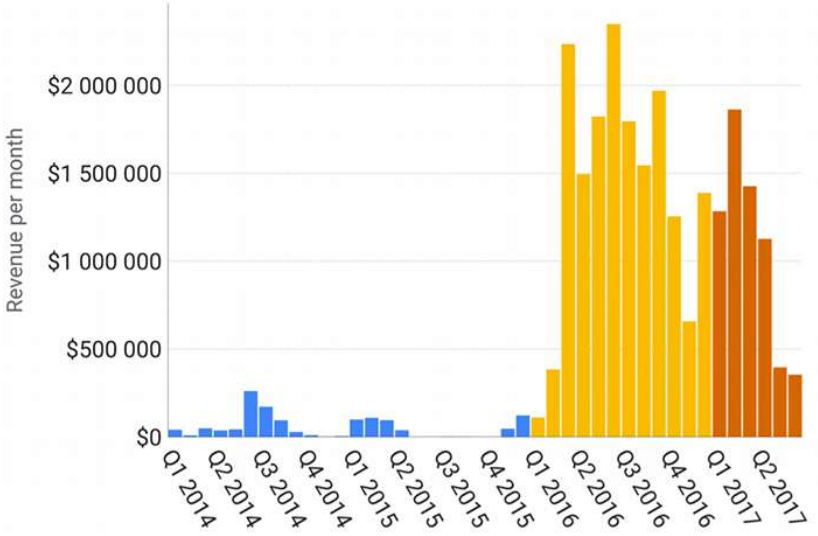


Figure 1: Monthly Ransomware Payments 2014-2017
Source: Google, UC San Diego, etc.

Ransomware	Period	Profit Evaluation
CryptoLocker	2013	~$3 million
Cryptowall	2014-16	~$18-$320 million
Locky		$7.8-$150 million
Cerber		$6.9 million
WannaCry	2016	$55,000-$140,000
Petya/NotPetya		$10,000

Table 7: Revenues from Selected Ransomware Products

"There is a distinction between ransomware products designed for revenue generation and those designed for disruption."

Higher estimates of ransomware revenues can be found in figures produced by the FBI, which suggested that ransomware payments for 2016 alone would reach around $1 billion (NBC, 2017). These contrasting estimate ranges are typical in cybercrime research, but what we can conclude is that whether it is $25 million or $1 billion, ransomware now offers a growing income stream for cybercriminals.

But as the revenue breakdown above suggests "the most profitable cybercrime" it is not. No matter how damaging or stressful it is to be a victim of ransomware attack, the profits here are still fairly small when compared to high income generators, like illicit online markets.

Nor is it clear that ransomware's primary function is always as a revenue generator. For example, researchers who have looked at high profile ransomware – like WannaCry or the Petya/NotPetya – found that monetisation of the ransom demanded has not been conducted very effectively. The implication being that there is a distinction between ransomware products designed for revenue generation and those designed for disruption – possibly at the behest of state actors.

Case Studies and Examples

Daewoo IP Theft

In 2009, the South Korean firm Daewoo discovered that over 6,000 computer files relating to a new sedan car model had been passed on by employees to Russian carmaker TagAZ. (U.S. Chamber of Commerce, 2015). Developing the car had cost around $245m. An injunction they filed was successful in preventing Tag AZ from using or disclosing any of the trade secrets.

Fruitfly Spyware Attack on Universities

In 2017, spyware dubbed 'Fruitfly' was detected in a range of U.S. biomedical facilities, especially within Universities, which targeted Mac computers. The malware enabled webcam access and screen grabs and was only discovered after unusual outgoing traffic was detected. To who/where and for what purpose remains unclear, but the high value of biomedical data provides some obvious motivations.

ThyssenKrupp Gets Hacked

In 2016, the German steel maker ThyssenKrupp discovered it had been hacked – possibly by the Winnti Chinese cyber espionage group. Technical trade secrets were stolen from its plant engineering division with significant – but undisclosed value. The attack is part of a general pattern suffered by German companies who usually have high value IP that is attractive to cybercriminals. A recent survey by Bitkom, the German industry association, suggested that over half of German companies have been victims of spying or data theft in the last two years, at a cost of over €55 billion per year.

Dark Web Houses IP Secrets in Norway

In late 2017, it was found that deep web sites were trading trade secrets belonging to a number of Norwegian companies. For example, the company Statoil reported that data relating to a wind power project

had been stolen and was subsequently found being sold on the dark web.

Spear Phishing Attack on Saudi Government

In 2017, 12 Saudi Government agencies were discovered to have been victims of espionage-directed spear phishing cyberattacks. The attack aimed to place malware on computers to mine or steal data from them. In the last few years, Saudi businesses, especially in the energy sector have also been victims of spying attacks from malicious actors such as the Greenbug cyber espionage group or the Shamoon hacking group, who were able to disrupt over 35,000 computers at the Saudi Aramco oil company in 2012.

Chapter 4: Laundering Dirty Money

Estimating revenues from cybercrime is only one challenge in attempting to follow the money. Unless we have a sense of how revenues are converted into forms that retain their value, whilst allowing them to be concealed or laundered, the trail is all but impossible to follow. As suggested in the next section on spending, some revenues appear to be disposed of fairly quickly. However, much of it is not and thereby requires ongoing ingenuity to find ways to conceal it for spending at a later date.

"Current best estimates suggest that cybercrime proceeds now constitute around (at minimum) 4%-10% of total global money laundered. This could amount to up to $200 billion of cybercrime revenues in circulation."

There have been various attempts to work out the volume of laundered money currently in circulation. For example, in 1998 the International Monetary Fund, suggested that sums of

up to 2-5% of the world's gross domestic product was being laundered, with a value at the time of between $590 billion-$1.5 trillion.

A more recent estimate provided by the UN (UNODC 2011) arrives at strikingly similar conclusions, suggesting that around 2-5% of total global GDP – up to $2 trillion – may now be circulating in illicit or laundered forms. But as awareness and controls on laundering have begun to supplement the role of banks and financial institutions in reporting uncharacteristically large deposits it has (in theory) grown harder for criminals to use the financial system to cash out their profits. But washing dirty money clean has been a perennial problem for any criminal enterprise, so it is not surprising there are some tried-and-tested means for doing this, which cybercriminals have been willing and able to exploit. In addition, newer methods presented by the digital economy, have also begun to emerge.

Traditional Laundering

More traditional methods of laundering that cybercriminals have used include:

- **Illicit Use of the Banking System**

  Being able to use legitimate banking systems to conceal money is clearly attractive since it can almost immediately make "bad money" good. This requires some form of complicity within banks or financial institutions and whilst this is unusual, the rewards can be great enough to tempt insiders at such institutions to lend assistance.

  In March 2017, British banks including HSBC, Lloyds, Barclays and Coutts found themselves under investigation

as a result of potential involvement in a huge Russian money laundering operation dubbed "The Global Laundromat" (Harding et al, 2017). Anything between £20-£80 billion was moved out of Russia between 2010-2014, and questions arose as to why these banks failed to report around 2,000 transactions from Moscow involving over £780 million as suspicious.

Given the ease of laundering where banks or bank staff cooperate it is hardly surprising that cybercriminals have quickly cottoned onto this as an option. In 2017, the U.K. National Crime Agency found that more than £16 million had been laundered for cybercriminals by a group of five men, including a corrupt banker working at Barclays. The group managed to set up around 400 bank accounts, which they used to filter stolen funds before transferring it back to cybercriminals in Eastern Europe (Sky, 2017). Similarly, evidence that banking staff have used dark web sites to pass on information, or to be recruited into scams, suggest that activity of this kind may be more prevalent than it seems.

- **Use of Shell Corporations or Fake Businesses**

  Shell or fake businesses can be used to convert dirty money into clean varieties. The recent growth of these entities as a way of shielding money has been significant. In the mid-1980s, less than 5,000 such corporations were registered in the British Virgin Islands – but by the mid-1990s there were over 120,000. The Cayman Islands had no such corporations in the early 1960s, but by 1995, there were 23,500 (Richards, 1998).

  The trend here is obvious enough and one would presume that cybercriminals with cash to spare will be no less willing

to make use of this option for concealing their revenues than other criminals. Hubbs (2014), reports that cybercriminals are now amongst the most frequent users of the scam, but hard evidence remains patchy. However, one recent case linked to the theft of over $5 billion bitcoins from the Tokyo Bitcoin exchange Mt Gox appears to support this idea. A U.K. registered firm, Always Efficient LLP, seems to have acted as a shell company for rival Bitcoin exchange BTC-e, which was closed down as a result of extensive cyber-laundering (White, 2018).

In order to regulate the use of shell companies, new rules require that a PSC (person with significant control) must always be listed. However, the most recent PSC listed for Always Efficient is a DJ in a Moscow nightclub who denies any knowledge of the business. That, and the fact that Always Efficient's address is shared by other companies suspected of money laundering, raises obvious suspicions about the legitimacy of the company and its role in concealing revenues acquired from Mt Gox that were subsequently laundered through BTC-e.

- **Investments in Financial or Other Assets**

  Hiding money by investing it in assets has been a very successful form of laundering. The aim is to transform a large cash amount into something less conspicuous, but which is equally valuable. This might be in financial assets or exotica like rare art or wine, but it can also include investment in property, land, or even energy and oil industries.

  Researchers have found evidence on discussion forums that cybercriminals are now actively looking at using financial

markets for investments, or even for generating new revenues, by stealing confidential data around mergers and acquisitions before using this to play the markets (Kuchler, 2014). During field work conducted for this research, it emerged that cybercriminals in the Caribbean specialising in romance frauds were making such significant investments in property in Jamaica that it was impacting upon the country's GDP.

- **Gambling and Casinos**

  The use of casinos has long been a favourite channel for money laundering. For example, it is a relatively easy practice to buy gambling chips and then sell them on or convert them into other forms. In one recent scheme, a launderer made a series of low-risk bets at various bookmakers within his city, resulting in a 7% loss rate. He then made out the cheques for the winnings to 14 bank accounts in the names of 10 different third parties and their families – some of whom just happened to be criminals (Reuter, 2005).

  The growth of unlicensed online gambling sites has provided a whole new area of opportunity for laundering cybercriminal's money. The online gambling industry was worth around $39 billion in 2016 (Cosgrave, 2014) and the sheer number of unlicensed sites (over 25,000, even in 2011) means that it is almost impossible for law enforcement to keep track of how money might be laundered through them. In early 2018, it emerged that up to five online casinos might lose their licences to operate in the U.K., after an investigation by the U.K. Gambling Commission found significant problems with their money

laundering controls – in particular, the failure to submit adequate information about suspicious activity (Davies, 2018).

- **Wire Transfers**

  Money can easily be moved from one jurisdiction to another using old-fashioned wire transfer services, such as Western Union. Cybercriminals have become adept at using these facilities to pay for stolen data, CaaS, or to purchase digital currency. Research in Nigeria (Panda, 2010) reported how they regularly used Western Union or MoneyGram to transfer funds, with one individual reporting that they preferred the former because: "…the Western Union agents themselves are all in the game, so you can claim your money with fake identity and they just collect 5% from you for themselves".

  In 2017, Western Union was ordered to pay $586 million by the U.S. Department of Justice to settle fraud charges. Over 550,000 complaints about fraudulent transfers were made to Western Union between 2004-2015; most related to cybercrimes, such as lottery scams, online romance and dating frauds, 419 and family emergency scams, and multiple instances of other illegal activities. Over $632 million was transferred as part of these frauds.

  The DOJ also found extensive use of Western Union for people trafficking and smuggling, with transfers of hundreds, up to millions of dollars made to China by illegal immigrants to pay the smugglers. Western Union appeared to be aware that illegal structured transactions were occurring and at least 29 convictions of owners or employees of Western Union have been recorded since

2001 (Paganini, 2017). Compelling evidence was found of significant transfers being conducted from known cybercrime locations, like Albania and Nigeria, to destinations around the world.

- **Money Mules and Cash Drops**

  Another very well-established laundering method has been the use of individuals to physically carry or receive criminal revenues – the so-called mule. The scale of money transferred in this way has led to numerous government and policing initiatives to prevent it. For example, a series of coordinated actions by Europol's EC3, the Joint Cybercrime Action Taskforce, Eurojust, and the European Banking Federation have supported the European Money Mule Action initiative. The second of these, in 2016, led to the arrest of 178 individuals and the identification of 580 different money mules across Europe. These suspects were linked with criminal activity resulting in €23 million in losses (Europol, 2016).

  There is emerging and fairly reliable evidence that this system is being extensively used by cybercriminals – whether for conducting transactions or laundering the revenues that have been obtained. A surprising finding of this research was the extent to which some cybercrime groups were physically transporting cash. At least 30% of a sample of interviews with convicted cybercriminals (n=100), reported that they physically transferred cyber revenues or sent money via couriers on airlines to deposit in foreign banks. And the European Money Mule Action initiative, discussed above, found that 95% of money mule activity had direct links with cybercrime activities.

Mules may be aware of the role they are being asked to play or they may be unconsciously duped, but either way they can be very successful ways in which dirty money can be made legitimate. The use of mules has been made a great deal easier by the slack rules in many foreign jurisdictions, where online accounts can often be opened with no need to present identification, or to actually appear at a branch.

In a sign of the plasticities between different areas of cybercrime activity, mule operations can also be used as a form of revenue generation. One of the most common and effective ways of updating mule forms of laundering used by cybercriminals has been via so-called "reshipping scams". Such schemes work by criminals purchasing products with a high value (usually with stolen cards or personal data). Individuals (aware or not) are then recruited to receive the packages and forward them on to the cybercriminals. Once they have been received, the product can be sold on the black market for cash. In just one operation tracked by researchers (Hao et al, 2015), around 6,000 packages were shipped in only the nine months the scheme was in operation. This brought in an annual revenue of $7.3 million and contributed to nearly $1.8 billion overall reshipping scam revenue (ibid).

Cyber-Laundering

Evidence of the use of traditional laundering methods by cybercriminals suggests how easily the needs of The Web of Profit can be adapted to the existing economy and is a further indication of the increasing interdependence between the legitimate and cybercriminal spheres.

However, these methods are now only one amongst many newer options for laundering. The shift towards digital payments, digital currencies, mobile payments and other new forms of exchange offer an emerging toolbox for moving and disappearing cyber revenues, some of which are reviewed below.

Use of Payment Systems Like PayPal

An important and growing feature of the cybercrime economy has been the development of electronic money and digital payment systems. These permit "cashless" transactions and can often be used with relative anonymity and often outside of traditional banking controls.

"PayPal and other digital payment systems were used as laundering tools in at least 20% of cases sampled for this research."

PayPal is perhaps the most well-known of these and there is ample evidence of its use both to commit cybercrimes – in particular, phishing – but also to launder revenues that arise from their commission.

Though prominent, PayPal is only one part of a very much larger shift towards the criminal use of such tools. There are now many other digital payment systems and forms of electronic cash, such as: Skrill, Dwoll, Venmo, Xoom, Popmoney, Square Cash and mobile payments systems, like Kenya's M-Pesa, which also offer opportunities for (mis)use by cybercriminals.

"Laundering methods using digital payment systems tend to be used in conjunction with a range of other methods, for example the use of stolen bank account details or other forms of identification."

The attractions of using a mobile phone as a virtual wallet, without having to depend upon finding a bank, are especially obvious – particularly in countries where banking systems are less developed. M-Pesa has been especially successful and has grown rapidly, with over 15 million subscribers now using it to transfer around $1 billion per month (GSMA, 2017). With that volume of digital money in circulation – and largely outside the traditional banking system – it is hardly surprising that the U.S. Treasury has recently warned that mobile payments systems, like M-Pesa, are likely to be one of the big growth areas for laundering.

Up to 3,000 cybercrimes a month are now reported in Kenya alone and there have been repeated attempts to hack into M-Pesa (Benyawa, 2016). Within the next couple of years there are likely to be 50 billion connected devices, and newer mobile payment systems – such as bKash in Bangladesh and Yellow Pepper in Latin America, amongst others – will be highly popular forms of banking, often in regions that are recognised cybercrime hubs.

Digital payment systems appear to be most effectively used for overt laundering activities when combined with online transactions, or as one part of a suite of other laundering methods and resources. A very common technique here is to use sites like eBay to make purchases that can facilitate the

laundering. These transactions are then able to pass through the PayPal system with less suspicion and the money received will conveniently disappear.

"The growing use of digital payment systems by cybercriminals to launder their revenues is helping erode both the autonomy and authority of the traditional financial system by generating significant revenue flows outside of its remit or jurisdiction."

However, traditional banking accounts, physical cash and, increasingly, cryptocurrencies like bitcoin are also often used as part of a growing portfolio of digital resources. These help to hide the trail of the money and to confuse law enforcement and financial regulators.

"Digital payment systems appear to often involve the use of micro-laundering techniques – multiple small payments made to evade laundering limits."

Covert data collection on online forums together with interviews with both experts and cybercriminals for The Web of Profit project indicated that in at least 10% of illicit activities or transactions, PayPal played some part in laundering revenues. Sums involved were sometimes up to around £250,000, despite PayPal having an annual receiving limit of €2,500. However, larger numbers (around 35%) of the sample, used less well-

known digital payment systems like those detailed above. The actual figures are probably much larger than what the hard data suggests.

Case Studies and Examples

PayPal Refund Scam

In one recent scam, cybercriminals exploited a PayPal feature that allows members to request money from one another. Members do this by completing a form that includes an area where they can enter a message. The cybercriminals used this feature to request a refund as a result of $100 being fraudulently sent from their PayPal accounts to the accounts of their intended victims. The plausibility of their claim was enhanced by including a goo.gl URL which ostensibly linked to documents that detailed the fraudulent transaction, together with an incident report that had been sent to PayPal. When the victims followed this URL, they were diverted to a website that used a disguised JPEG file to place a malicious script on their computers. Anyone who opened this file then found their computers became infected with malware.

PayPal Account Takeovers

Another recent case demonstrates a very common and more straightforward way in which PayPal can serve the ends of cybercriminals – as a tool for account takeovers. Following the recent takedown of the *InFraud* criminal platform over 1,300 compromised PayPal account IDs were found that were being offered for sale.

PayPal Accounts for Sale

There are numerous examples of dark web sites offering the sale of PayPal accounts. Scans conducted for this research across hacking forums found that 100 PayPal accounts could be obtained for around $100, or 0.4 bitcoin, on average.

PayPal Exploited in Israel

The Israeli hacking services group VdOs, which made over $600,000 during a two-year period, were found to have used PayPal for collecting revenues and laundering them before switching to bitcoin payments made through Coinbase.

PayPal and Online Drug Sales

One of the most notorious recent uses of PayPal for laundering involved a range of online drug markets that were in existence before the closure of the Silk Road marketplace. Amongst these was TFM (The Farmers Market), which sold everything from marijuana to ketamine. It not only accepted payments via PayPal, but also Pecunix payments (a digital currency like I-Gold), which had been laundered through PayPal (Power, 2013).

PayPal Micro-Laundering

In 2013, Jason Hagen, who sold Methamphetamine via Silk Road was also found to be involved in an extensive money laundering operation involving PayPal. Hagen received over $600,000 in payments, mostly using bitcoin and then diverted these through multiple PayPal accounts, fraudulently opened bank accounts and Western Union transfers to distribute his profits.

Hagen's method of utilising multiple PayPal accounts, or multiple deposits of small amounts, is widely used and draws upon techniques already been developed in legitimate banking circles. For example, during the huge HSBC laundering scandal where inadequate controls permitted billions of dollars to be laundered through the bank by organised drug gangs and rogue nations like Iran, testimony from whistleblowers indicated how PayPal was utilised by bank employees to launder cash. The process began with multiple transfers of amounts as small as 15 cents, sometimes over a period as long as 60 days. Once established, tens and hundreds of thousands of dollars were laundered through these multiple PayPal accounts.

Numerous examples of this technique, also known as “micro-laundering”, was examined in research conducted for the UN (Richet, 2013). “This showed how instruments like virtual credit cards, or scammed bank accounts, linked to PayPal accounts, permitted large amounts of money to be moved in small amounts by way of many thousands of electronic transactions”.

PayPal and U.S. Election Tampering

One of the most serious cases of PayPal being misused for deceptive purposes has only just emerged as part of the Robert Mueller investigation into attempts by Russia to influence the 2016 U.S. Presidential election. Following the indictment of 13 Russian nationals it has emerged that authentic U.S. social security numbers were stolen and used by the Russians to open PayPal accounts which, in turn, provided fake IDs for them to open Facebook and other social media accounts.

PayPal and Terrorism

At the very extreme is the misuse of PayPal for laundering terrorist financing. A recent example here involved an ISIS operative based in the U.S., Mohamed Elshinawy. Following an oath of allegiance, Elshinawy received around $9,000 from the organisation through PayPal. The money was concealed using fake computer printer sales on eBay.

PayPal Losing Its Appeal

PayPal is now very much only an entrée to the world of digital money laundering and there are many signs that sophisticated cybercriminals are exploring a far wider range of digital payment systems. Conversation data obtained from observations of dark web sites for this project indicated a clear awareness amongst cybercriminals that other digital payment systems may now be safer and more productive options. This included comments like:

– “I will stop using PayPal within the next month and a half. ccnow is a much better option and they do not share any information with

eBay/PayPal. It's also great because you can accept PayPal payments through ccnow."

- "Buy gold and sell it on eBay instead – much easier."
- "If you want fool proof then prepaid is still a good option, but you can go on Venmo and reverse the transaction."
- "I never use PayPal anymore, the feds are all over it these days."

Anonymous Transactions Gaining Momentum

A clear example of the shift towards alternative digital payment systems for laundering can be seen with the recent case of the digital currency service Liberty Reserve, based in Costa Rica. Its capacity for enabling anonymous transactions permitted laundering of over $6 billion around the world. Many of these transactions were blatantly criminal. Transferring money using Liberty Reserve only required clients to supply a name, address and date of birth, with no other validation for their identity. This permitted numerous accounts to be opened using fictitious IDs – sometimes with names like Russian Hackers. Investigators were also able to open accounts, listing their purpose as things like "for cocaine".

Use of Cryptocurrencies for Laundering

The growth of Bitcoin and other cryptocurrencies as contributors to both the licit and illicit economy has begun to be widely acknowledged and observed. With over 15 million total bitcoins now in circulation and more than 150 million total Bitcoin transactions logged so far (comprising up to 250,000 transactions a day); Bitcoin is very much at the centre of the growing virtual currency marketplace. One major Bitcoin wallet provider – Blockchain – manages more than 12 million wallets, which represents a twelve-fold increase since 2014 (Carlisle, 2017). But even with this volume of transactions, bitcoins and

other cryptocurrencies remain a phenomenon very much at their inception with cash transactions still by far in the majority.

"Indications are emerging of a shift away from Bitcoin by cybercriminals to less high profile, less trackable systems like Monero."

At present, opinions vary on how significant cryptocurrencies really are for laundering. The U.K. National Crime Agency remains sceptical about the scale of this – and Europol agrees that "cash remains core to money laundering" (SOCTA, 2017). Others are convinced that Bitcoin and other cryptocurrencies represent the future of money laundering (Khan, 2016).

It was clear from this research and from other sources that Bitcoin's moment in the criminal sunshine may be declining in favour of other types of cryptocurrency. One reason why many cybercriminals have begun to avoid Bitcoin relates to the transparency of the blockchain and the increasing number of tools for detecting how funds are transferred via Bitcoin wallets.

"Direct transfer systems like the Islamic Hawala system are offering particular laundering opportunities since they are peer-to-peer forms of exchange, operating outside of the usual controls."

The use of mixers or tumblers (software that can obscure the blockchain) represents one attempt to get around this can

arbitrate against this, with recent research suggesting that 25% of Bitcoin transactions are put through mixers (Robinson & Fanusie, 2017).

However, the recent decision by Dutch authorities to charge anyone using a mixer is likely to pose some serious challenges in trying to obscure their use. Other factors such as the volatility in bitcoin values and potential trading bans in jurisdictions like China and South Korea, is also reducing its appeal. The likely affect has been to shift attention towards newer cryptocurrencies, such as Monero. As well as providing encryption for the recipient's address on its blockchain, Monero can produce false addresses to hide the actual sender and can hide the transaction amounts.

Case Studies and Examples

Bitcoin ATMs Provide Easy Access

One of the most common and low-key ways in which Bitcoin is used to launder money is by way of bitcoin-specific ATMs. This is now becoming a useful tool for traditional criminal activities. Evidence collected during this research and subsequently confirmed in the media, suggested that Bitcoin ATMs located in corner shops or other low-key sites in London, U.K. were being used by drug dealers and prostitutes to turn their hard cash profits into less easy-to-trace digital forms.

This pattern is one that appears to be being replicated across the world. Another police intervention in 2017, this time in the U.S. State of Utah, found that a drug gang was using bitcoins to launder substantial parts of their profits. The operation was broken up by law enforcement and their bitcoin assets were seized.

Silk Road Conviction

One of the largest and well-known cases of the connections between online markets, drugs sales and bitcoin laundering, is the conviction of the Silk Road's Ross Ulbricht. U.S. police say that they seized over $28 million in bitcoin from Ulbricht, which had been used to launder the huge profits made from the online drugs market. Somewhat ironically, U.S. police have subsequently auctioned 50,000 of the laundered bitcoins (which in April 2018 was worth over $300 million).

In 2017, Shaun Bridges, a secret service agent involved in the prosecution of Ulbricht was himself sentenced to six years, following attempts to launder over $800,000 of bitcoin he had diverted to his accounts.

Argentine National Scams with Bitcoin

A 2014 case involved an Argentine national who was arrested in Barcelona after being discovered running a device to falsify credit cards and tickets on the public transport system. He also ran a scam involving the sale of Euros in exchange for bitcoins. Buyers never received their coins, but the criminal was able to use his schemes to generate over €1 million, which he laundered into bitcoin.

Dutch Nationals Get Caught Laundering

In 2016, 10 Dutch nationals were arrested after trying to launder up to €20 million from drug trafficking proceeds, by selling these on the black market using bitcoins. Their operation only came to light after they tried to cash out bitcoins that had been converted to bank accounts then cashed out through ATMs.

Sheep Online Drug Market

In March 2015, $40 million in bitcoin was laundered by 28-year-old Czech national Tomáš Jiříkovský, who ran the Sheep online drugs market. Transfers had been made from an account registered to Jiříkovský on the Bitstamp bitcoin exchange to his girlfriend's account.

WannaCry Used Bitcoin and Monero

In September 2017, a trend emerged that suggested that cybercriminals were converting bitcoins into other cryptocurrencies that were easier to hide. An Italian security firm, Neutrino, was able to track how revenues totalling between 5 bitcoins to 51.93 bitcoins, gathered from the WannaCry ransomware, had begun to be converted across from Bitcoin to Monero.

E-Gold and WebMoney Used for Laundering

In 2013, in New York, the president of a virtual currency exchange for E-Gold and WebMoney, called Western Express International, Inc pleaded guilty to money laundering. U.S. Secret Service agents found that stolen credit card information, which had been exchanged by hackers for E-Gold and WebMoney, was being converted into dollars using Western Express. Over $15 million in WebMoney and $20 million in E-Gold had been converted.

In 2008, an administrator for the E-Gold digital currency, along with the three principal directors and owners of E-Gold Ltd, were found guilty of money laundering and of running an illegal money transmitting business. All that was required to open an E-Gold account was a valid email address. Account holders, irrespective of location, could engage in anonymised online transactions by a simple transfer of E-Gold from one account to another. Evidence from the trial suggested that E-Gold had become a favoured method for cybercriminals for purchasing stolen financial information and child pornography.

Columbian Drug Smugglers Use Bitcoin

Elsewhere, evidence is emerging of more serious uses of bitcoin as a criminal enabler, beyond its role as a laundering device. For example, recent U.S. intelligence has suggested the use of bitcoin in Columbian drug smuggling and has identified instances of human traffickers accepting bitcoin for online sales. In a testimony to the U.S. Senate Judiciary Committee, an agent in charge of Homeland Security Operations for Immigration and Customs Enforcement pointed to the

use of bitcoin by child smugglers and exploiters as well as drug smugglers and IP violators for criminal transactions.

Cryptocurrencies appear to be well suited to laundering for a number of reasons. Firstly, they are digital – and therefore easily convertible ways of acquiring and transferring cybercrime revenues. Secondly, they were initially perceived to allow anonymous transactions. But, as discussed, the blockchain technology behind Bitcoin and other cryptocurrencies means that all transactions are transparent; even though those using it, in theory, are not. Thus, numerous tracking apps, like the one seen below, were set up in the wake of the WannaCry and Petya families of ransomware, to follow bitcoin ransom payments as they came in and out of designated wallets.

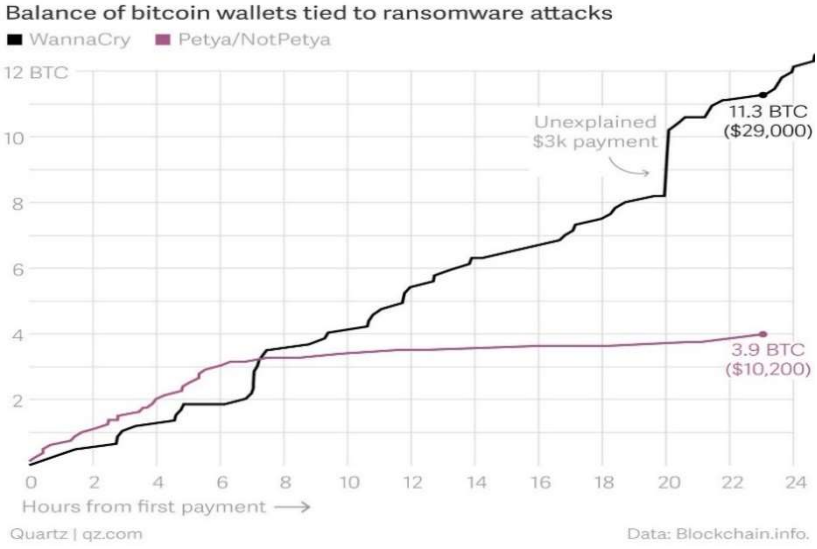


Figure 2: Bitcoin Wallets Tied to Ransomware Attacks

Even tumbler or mixer services, such as CoinJoin, or CoinSwap, which are used to obscure the origins of payments (by allowing users to mix their Bitcoin payments to make it harder to identify them), may not always succeed in concealing them. Aside from the possibility of legal controls of the kind created by The Netherlands that were discussed above, there are other more technical drawbacks for their criminal use. Researchers at Princeton have found that the information that inevitably leaks out during web interactions – via web trackers and cookies, for example – suggests that a unique linkage to individuals is possible in upwards of 60% of Bitcoin transactions (Goldfeder et al, 2017).

"Laundering through cryptocurrencies remains relatively small compared to the volumes of cash laundered through traditional methods."

Alternative cryptocurrencies, like Monero or Zcash, have been designed more with anonymity in mind and cybercriminals appear to be increasingly interested in using them, rather than Bitcoin. For example, in 2017 the ransomware package Kirk was the first to use Monero as a payment mechanism (IOCTA, 2017). But even here, there remain ways for law enforcement to track payments, though these remain covert at present.

Laundering through cryptocurrencies remains relatively small compared to the volumes of cash laundered through traditional methods. For example, a Europol estimate has suggested that money laundered via cryptocurrencies was only up to 4% of the total laundered in Europe at present (Silva 2018). However, it is undoubtedly the case that we are at the

beginning of an arc, rather than at its end. The complex economic structures developing around cyber-criminality mean that cryptocurrencies are only likely to enhance criminal capacity within The Web of Profit, rather than diminish it. And this implies that illicit uses of cryptocurrencies will continue to grow. This is evident in the many stories that are beginning to emerge around the role of cryptocurrencies in enabling the conversions and transfer of funds.

In 2016, for example, Dutch police arrested 10 individuals following the deposit of large sums in banks, before being immediately withdrawn from cashpoints. This appears to have come from sales of bitcoins (Guardian, 2016). Elsewhere, in 2017, one of the highest profile arrests connected to bitcoin laundering came with the arrest of Alexander Vinnick in Greece (Popper, 2017).

Vinnick has been charged with using the cryptocurrency exchange BTC-e to launder around $4 billion in bitcoin for cybercriminals and other individuals involved in criminal activity (a charge he denies). But BTC-e customers who used pseudonyms like CocaineCowboys, ISIS and dzkillerhacker were not required to provide identification when opening new accounts, making it easy to launder bitcoins harvested from online crime. It is estimated that 95% of ransomware profits have been cashed with BTC-e, making it one of the largest cybercriminal laundering operations (Fox-Brewster, 2017).

"The scale of laundering through games, though suspected to be growing, remains poorly understood, with minimal data available."

The idea of using currencies hidden within computer games that can be easily converted into other cash forms and which enable transfers across international borders with little scrutiny, is clearly an attractive one. How much of an actuality this is at present remains to be seen, as evidence has been either limited or anecdotal to date. This has not prevented the U.S. financial regulator FinCEN from issuing guidelines making it clear that, for laundering purposes, any individual or company involved in currency exchanges in games can now be considered a money transmitter and prosecuted accordingly.

"Laundering via gaming has been significantly extended by the increased use of in-app and in-game purchases."

The growth of in-game purchasing has added a suite of extra possibilities for laundering which now go beyond the misuse of straightforward currencies, or items like gold. At present, the number of gamers who engage in such purchases appears to be fairly low, with recent research suggesting that just 0.15% of players were responsible for half of in game revenues (Takahasi, 2014). However, this exclusivity may also add to its criminal appeal.

"Far East countries such as China and Korea are hotspots for in-game currency laundering."

There is a growing awareness amongst gaming companies of the risk that cybercriminals involved with card theft or laundering may be creating websites where frauds can be enacted. The company Kabam – which publishes games such as Kingdoms of Camelot, and Star Wars: Uprising – recently issued a warning about the possible misuse on third-party websites of Mithril, the gaming currency used in its Hobbit game:

> *"We have seen a surge of activity from fraudulent third-party sites that are not affiliated with Kabam, claiming to sell cheap Mithril for various Kabam games…the use of these sites may compromise your game and payment information. These web sites use stolen credit card information to make the Mithril purchases that you would receive. This opens you to potential fraudulent activity in the future"* (Szabo 2016).

Case Studies and Examples

Korean Gold Farming in Gaming

In 2008, Korean police arrested members of a money laundering gang who were assisting a Chinese "gold farming" group (collecting high value gaming items.) They were attempting to transfer over $38 million gathered from online Korean games back to China.

MMORPGs Like Minecraft Used for Laundering

Research into online gaming laundering in 2013 (Richet 2013) found a variety of sites offering information on how to launder money through

gaming currencies. Especially common was the role of MMORPGs (massively multiplayer online role-playing games) like Minecraft, which allow players to interact across differing jurisdictions and to exchange currencies with limited international controls. Data was gathered from a number of forums where advice was freely offered on how to do this. For example, one report suggested buying as many in-game assets as possible and then creating a black market to sell them in order to convert cash. Others suggested more established gaming gold markets. Even though commissions are taken there, conversions are largely reliable.

Dark Web Gaming Forums Attract Laundering

Observations conducted on three dark web gaming forums found references being made to games such as Clash of Clans and World of Warcraft as options for disappearing funds. New sites such as MmoGah were cited as offering easy ways of converting gaming gold or currencies to real cash, though because of regulations there, covert sites on the dark web were indicated as preferable.

A variant of these techniques was found in China, where revenues were used to buy gaming credits, which could then be sold for cash.

Chapter 5: Disposing of Criminal Revenues

Determining how criminals spend their profits presents one of the most challenging current knowledge gaps in our understanding of cybercrime – for police and government, as much as for researchers. A key problem here, whether looking at the disposal of revenues in traditional crime or in cybercrime, is where to obtain data from and how to *interpret* whatever can be obtained. And one of the few sources where such information might be obtained – criminals convicted of, or engaged in, cybercrime has obvious problems with reliability. Criminals may be unwilling – or unable – to provide trustworthy information for various reasons:

- Others involved in their crime may still be spending the profits.
- They may have received threats should information be revealed.

- They may wish to spend or reuse profits when they are released.
- General antipathy – they may simply wish to lie or to make life difficult for law enforcement or other investigating agencies.

Other sources of data – such as the Asset Forfeiture Program in the U.S. or court records about confiscations under the U.K. Proceeds of Crime Act (POCA) – are not always easy to access. Such data may also be misleading, since it is not always clear what involvement cyber-criminality has in any case where assets are seized.

If the spending patterns discovered in the sample of convicted or active cybercriminals interviewed for this research were to be replicated at the level of global $1.5 trillion revenues determined here, this would imply that:

- Up to $300 billion of cybercrime revenues are now being reinvested into further criminal activities, either to fund new or existing cybercrimes or for other, potentially more serious offending such as terrorism or trafficking.
- Up to $450 billion of cybercrime revenues are being invested by cybercriminals in financial, property or other assets. This is likely to be having increasingly significant impacts upon the way the legitimate economy functions.
- Up to $750 billion of cybercrime revenues (around 50% of the total) is being spent by cybercriminals on status-seeking, hedonistic, or otherwise mundane purchases. This volume of spending and the likely casual nature of some of it presents law enforcement and other regulatory agencies with significant options for intervention or disruption.

Some caution is required, however, in extrapolating these totals on the basis of the sample interviewed. Given the possibility of sample bias in the types of offences cybercriminals interviewed were responsible for, it cannot be automatically assumed that cybercriminals involved in other kinds of offending would spend revenues in exactly the same way. More data would be required to be able to firm up these assumptions. However, even as a preliminary observation, there are clearly some significant conclusions about the impact of cybercrime revenues upon cybercrime activity that can be drawn. It is to be hoped that by acquiring more data of this kind, researchers will be able to develop such inferences with greater precision.

In spite of such limitations, researchers have nonetheless been able to piece together some of the ways in which traditional criminals spend their cash. For example, a recent U.K. Home Office study (Dubourg & Prichard, 2008) attempted to get some sense of the patterns here by looking at the kinds of areas in which criminal assets were stored. Of all assets:

- 69% was in the form of property.
- 11% was found in bank or building accounts.
- 8% in other financial assets.
- 1% was in the form of vehicles.

This finding has interesting implications for the impact of criminality upon the legitimate economy, with around 1-2% of annual property transactions directly funded by criminal gains. For example, in the U.K., by linking this to tax and revenue data (from the HMRC), we can see that this equates to roughly

150,000-300,000 properties each year, worth around £3.0-£7.4 billion – a sizeable investment by criminals.

A study by Kruisbergen et al (2014) developed a still more robust methodology for looking at disposals by organised criminals. It found some similar patterns. The research drew upon a data set of around 1,196 assets seized from (suspected) organised criminals. Suspects were variously involved in offences such as drug trafficking or production, people trafficking, illegal arms trading, as well as fraud and money laundering. Here too, there appeared to be a readiness to spend proceeds on investments like real estate or company investments. However, the study also indicated that suspects utilised their revenues to engage in substantive and conspicuous consumption, acquiring items such as expensive cars, boats, jewellery or spending money on holidays and their partners.

This pattern is also replicated in data obtained from the Russian operation global laundromat (Harding et al, 2017) discussed earlier. An analysis of revenue disposals during this operation clearly shows a similar predilection for luxury spending. For example, large amounts of the laundered money was used to buy items like diamonds, crystal chandeliers and expensive furs. Crime revenues were also used to fund one of the perpetrator's son's boarding fees at the prestigious Millfield School in Somerset, U.K..

Disposing of Cybercrime Revenues

Given the difficulties in analysing the revenue spending patterns of traditional criminals, it is not surprising that evidence for the ways cybercriminals spend their proceeds remains even sparser. Accordingly, this project – one of the few

studies of this kind – has had to draw its conclusions from limited sources across the cybercrime evidence spectrum.

Initial data was drawn from a sample (n=100) of interviews with convicted or active cybercriminals and from observations across a number of dark web and open web sources. Findings here were then filtered and compared against expert interviews, academic research, court and policing documents and whatever was available in the public domain.

The conclusions drawn are thus provisional and await further data collection and refinement by future researchers. But they do at least represent one of the best guesses that can be made at this point about some of the ways in which cybercriminals are disposing of their revenues.

How Many	What They Bought
15%	Used money to cover immediate needs
20%	Focused on disorganised or hedonistic spending
15%	Spent on status items to impress girlfriends, other criminals, etc.
30%	Converted money to assets like property
20%	Some portion spent on reinvestments in further criminal activities

From the data gathered, there appeared to be five broad areas where cybercriminals were most likely to be directing their spending.

They are divided as follows:

- **Spending on Immediate Needs**

  Spending largely related to maintaining a comfortable or adequate lifestyle. This can involve paying bills, running a car, purchasing food and other necessary items.

- **Disorganised or Hedonistic Spending**

  Spending that may be impulsive, or that involves unnecessary items oriented around the satisfaction of pleasures. This may involve anything from purchases of drugs, prostitution, or luxury, expensive items like sports cars or jewellery.

- **Calculated Spending**

  To some extent this dovetails with the previous category in that it may involve high-end or luxury spending. But here, the motivations are more centred upon acquiring or gaining status – whether amongst fellow criminals, partners and family, and so on.

- **Investment Spending**

  This involves spending directed at preserving or growing the revenues that have been acquired. For example, in property, financial instruments, or other items that hold value, like art.

- **Reinvestment in Crime**

  In terms of crime prevention, this clearly represents one of the more important spending categories. For it is here that law enforcement might profitably direct efforts to disrupt or prevent future cybercrime activities. However, re-investment is somewhat a term of art, since there may be many varieties of spending that could fall under this rubric

and it is not clear how justified it is to treat them in similar terms. For example, can buying a USB stick to save stolen credit card numbers on be equated with purchasing a suite of computer servers for directing attacks to obtain credit card numbers?

For the purpose of this research, a wide and inclusive sense of reinvestment was used, which includes spending on any item likely to make a significant contribution to the commission of further crimes. Thus, buying a cup of coffee to improve concentration during a DDoS attack would not count. Spending on any item of IT, however small, would.

Note that the above categories are not mutually exclusive, so the percentages indicated do not form a composite total. In other words, most offenders will cross between categories. For example, clearly all cybercriminals will spend at least some revenues on their basic needs and most will indulge themselves in at least some reward for their criminal endeavours.

"Transactions…are easy – and even more importantly, can be conducted largely out-of-sight from financial regulators."

In at least 30% (n=35) of the cases sampled for this research, cybercriminals reported attempting to convert some of their revenues into hard cash. When this happens, it is usually almost impossible to determine where the money goes next, or what they spend it on. As with traditional crime, physical money often creates a kind of black hole into which revenues disappear. All the more crucial, for researchers or law enforcement more generally, is to identify cashing out points –

nodes in the revenue flow where revenues that have been laundered are converted into physical or other assets.

The cash out barrier remains as much of a problem for cybercriminals as it has been for traditional criminals. No matter how ingenious the methods of moving money around might be, there is no ultimate reward in subterfuge alone. At some point, the revenues generated by cybercrimes will need to be converted into an end product, or at least assets that hold value. The cash out problem holds particularly strongly for revenues held in in cryptocurrency forms, since any move to transform them into physical cash can be quickly noted by financial or law enforcement agencies.

One way in which the cash out process from virtual currency to physical asset can be managed more smoothly is by way of *direct* conversion of currencies into assets. This tendency can now be facilitated by way of a variety of tools for instant conversion. Perhaps most straightforward are various websites that have sprung up that allow purchase of various assets and commodities – usually at the luxury end of the market – in cryptocurrency form.

Take, for example, the website below (see Figure 3), which offers a range of high-end land and property assets across the world, including penthouses in Paris and tropical islands. Transactions on the site are easy – and even more importantly, can be conducted largely out-of-sight from financial regulators.

Around 25% of payments for property are now predicted to be in cryptocurrency form within the next few years (Machalinksi, 2017). This prospect has concerned some financial analysts, who are worried about possible disruptions to the global property market as cryptocurrencies enable swifter, more covert property transactions, many with criminal origins.

Figure 3: http://bitcoin-realestate.com

The direct conversion of cryptocurrencies into physical assets is not, however, restricted to property. Many other online marketplaces now exist for direct disposals of such currencies into high value commodities. For example, some sites (see Figure 4) offer conversions into watches and jewellery, others allow direct purchases of cars using bitcoin (see Figure 5).

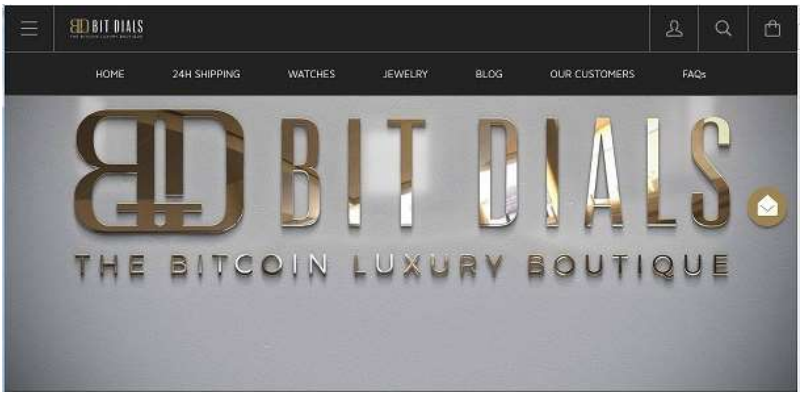


Figure 4: https://www.bitdials.eu/

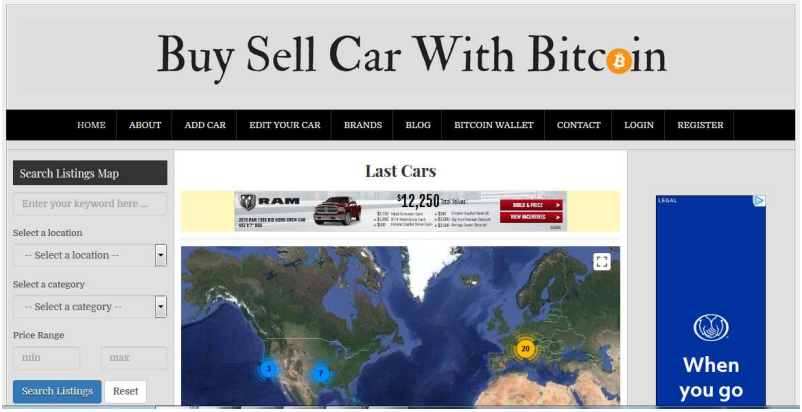


Figure 5: https://www.bitdials.eu/

Elsewhere, there are even options for converting cryptocurrency-based cybercrime revenues into assets like gold bars or fine art (see Figure 6). There are also increasing opportunities for purchasing items like hotel accommodations or computers via more traditional traders like Expedia or Dell.

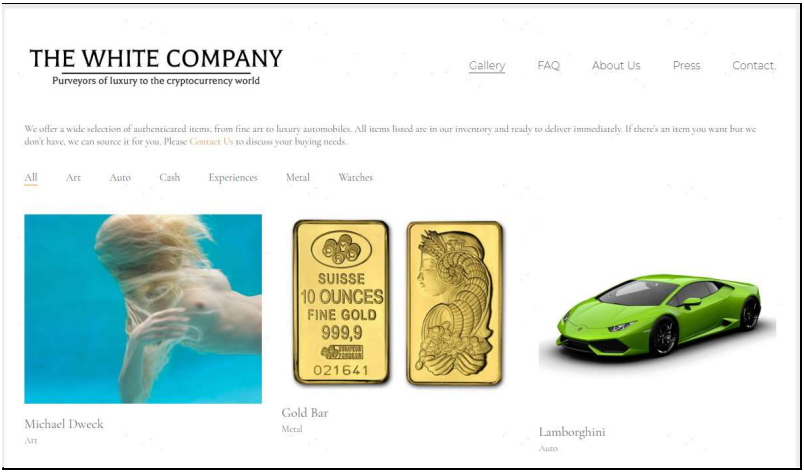


Figure 6: http://thewcomp.com

The pattern of spending cybercrime profits on high-end goods appears to be replicated when we drill down into data at the level of individual criminal consumption. Whilst it is, of course, hard to be definitive about the ways such revenues are disposed of here, triangulation across as many sources as possible – from interview data with suspects, to anecdotal reports in the public domain – allows us to build up a picture that offers some preliminary insights.

One more readily accessible and reasonably reliable source relates to spending patterns effected by the use of stolen credit card data by cybercriminals. One very large recent survey of this kind by the fraud detection company Forter, looked at over three million attempted transactions using stolen credit cards (Anand, 2015). This indicated a clear preference for luxury goods like Rolex watches, luxury hotel breaks or high status electronic goods, like MacBook Airs. This pattern was replicated in data obtained for the U.S. National Retail Survey (Fahmy, 2010) and in the sample data obtained for this research, which also found a readiness to engage in 'shopping sprees' for popular brands that could be resold on the internet or in street .

At the same time, there was also a readiness to use the stolen card data to purchase relatively mundane staples, like pizza. This too was corroborated in the field research for this project. Many of the cybercriminals interviewed who work at a more individual, spontaneous level tended to display impulse-driven patterns of purchases aimed at satisfying immediate wants and needs; rather than carefully considered long-term investments. In addition to lavish takeaway meals, there was also evidence of spending on prostitutes, cocaine or ostentatious gifts for those the criminal wished to impress.

Forter Study, 2015	U.S. National Retail Fed., 2010	Research Sample
Luxury goods		
Rolex watch	Braun toothbrushes	Sports cars
Louis Vuitton handbag	Claritin	Luxury spa weekends
Diamond engagement ring	CoverGirl cosmetics	Perfumes
Electronics and Digital		
MacBook Air	X-Box	Tablets
Smartwatch	Duracell Batteries	Smartphones
Device cases	iPods	Memory cards
Best Buy gift card	Gift cards	Gaming currencies
iTunes vouchers		
Food and Fun		
Pizza	KitchenAid Mixers	Prostitutes
Red Bull	Enfamil baby formula	Cocaine and other drugs
Luxury hotel rooms	Lingerie	Gifts

Table 8: Criminal Impulse Buys

Case Studies and Examples

Bad Guys Are Strategic

Interview data suggested that there was a strong correlation between the way revenues were predominantly spent and the level of professionalism involved in the offending. Where unnecessary risks were taken, or the operations were sporadic or 'one-offs', spending tended to be for immediate needs or for pure hedonism. For example, one individual who engaged in a one-off insider fraud that involved stealing customer card details at a small business where he worked, said that he had done it purely to pay off a series of debts.

By contrast, a more organised group engaged in auction frauds were observed discussing how they might disguise their revenues in the form of investments that were likely to hold their value and unlikely to attract the attention of law enforcement – for example, expensive wines or antiques.

Hedonism is Alive and Well

One example of largely hedonistic spending patterns can be seen in the habit of two individuals from York, U.K. who were convicted in 2017 of running an online drug supermarket selling fentanyl. The individual who masterminded the scheme received bitcoin payments worth between £275,000-£1.5 million, and police discovered that though he had bought some gold, he had spent a large part of his earnings on drugs, expensive watches and around £2,000 a week on prostitutes.

Living a Luxurious Life

A similar, though more directed pattern was also seen in the case of an individual who used a variant of the Zeus botnet to steal funds from around 127 U.S. banks. When asked by the police how he had spent his profits, he said that it was largely on travelling and living a luxurious life – for example, staying in five star hotels.

Living Large in Vegas

An online drug dealer in Wales who made over £2.5 million ($3.5 million) from his website used the revenues to fund a lavish lifestyle. Police discovered he had spent his profits on luxury experiences like a five-week holiday to Las Vegas where he hired Porsches and Lamborghinis at over $6,000 a time and gambled over $40,000 in casinos (Wales Online, 2015).

African Cybercriminal Surrounded by Suitcases of Cash

In 2017, an African cybercriminal who engaged in bank frauds and who attempted to hack into the mobile payment system M-Pesa was discovered to be living an extremely expensive lifestyle. As well as being surrounded by suitcases filled with dollar notes, he was photographed posing in designer suits and wearing expensive watches.

Czech Criminal Focuses on Investing

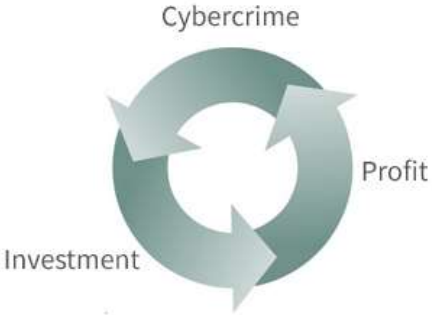
An example of more directed, investment-oriented spending can be seen in the spending habits of the Czech cybercriminal Tomas Jiříkovský, mentioned above, who made significant investments in property with his profits from the online drug market Sheep.

Gift Cards Used to Revenue-Up

Another permutation seen in the research was for profits to be invested back into crime. In one example from a previously unreported U.S. federal case in Florida, profits from stolen credit card data were used to purchase 45,000 gift cards for Walmart and other stores. These were then used to generate further criminal revenues through sales on the gift card exchange site Raise.com. The value of the gift cards, which ranged from $2 to $2,000 each, generated a total of $9 million of new revenues on Raise.

Reinvestment into Crime

A major gap in our knowledge at present concerns the extent to which revenues from cybercrime are reinvested into further criminal activity. If the revenues being generated are near the scale that this report has identified, then the potential for significant criminal enhancement is there – a prospect that has begun to alarm lawmakers (SOCTA, 2017). If these preliminary indications are correct, further research to understand just how criminogenic cybercrime is now becoming – that is, how far it supports, funds or enables further offending (whether in the cyber world, or beyond) – is clearly an urgent priority.



The most obvious variety of criminal investment into which revenues can be directed is into further cybercrime. If effectively functioning, cybercrime-loops that link revenues to specific crimes could be detected. This would clearly be of great significance for law enforcement and policy makers, since it would provide a range of obvious engines that drive the cybercrime economy.

There is evidence that something of this cycle, if not already in place, is starting to manifest itself. For example, many of the larger cybercrime operations that have been detected seem to have usually channelled at least some of their revenues into expanding and developing the operation – whether for buying further crimeware, maintaining a website, paying mules, or other criminal requirements. Given that one of the attractions of cybercrime is supposed to be its low start-up cost, it clearly need not require major investment to maintain or expand the scope of the offending with more sophisticated infrastructures.

In the Forter study cited above (see Table 8), there was evidence that stolen credit card data was not used merely for disorganised or hedonistic spending. Revenues here were also spent on investments in business-related activity, such as hosting services, remote hosting or logo and website design. Spending was also recorded on promotional aspects, such as search engine optimisation or coupons for Facebook ads.

Equally (if not more) serious, would be for cybercrime revenues to be directed towards sponsoring other varieties of crime. And though the evidence base remains limited, there do seem to be enough indicators to suggest that something like this is occurring. Drug production and drug trafficking present some obvious and immediate examples of this trend. Recent research by Europol (2017) indicated just how intertwined the drugs market already is with organised crime, with around 35% of organised crime groups in the EU alone directly involved in the production or trafficking of illegal drugs.

"There is even evidence that groups that acquire revenues from cybercrime are involved in the active production of drugs."

Drugs represent the single most profitable criminal market in the EU with revenues – at the very minimum – of around €24 billion per annum. We know that up to 57% of dark web activity is now associated with trading in drugs, so it seems obvious enough that at least some of the significant profits from online drug markets will be reinvested in operations – if only to purchase enough new stock to permit further trading. Cybercrime tools of this kind have significantly furthered the spread of new psychoactive substances with over 620 new synthetic drug types on the market since 2005 (Europol, 2017). Many substances of this kind are manufactured in China or India, purchased via online markets, then shipped in bulk to Europe.

There is even evidence that groups that acquire revenues from cybercrime are involved in the active production of drugs. For example, the arrest of the Dutch money laundering gang discussed earlier (Guardian, 2016) also led to the discovery of ingredients they possessed to make ecstasy – further highlighting a material link between cybercrime activities and organised crime activities.

Establishing the existence of revenue flows from cybercrime into other criminal activities is harder, but there are good reasons to suppose that something like this is occurring. For example, we know that there is a sophisticated relationship between revenues from prostitution – especially in its new online forms – and the problem of people trafficking. Pimps

frequently use the internet as a tool for gathering revenues from clients and workers, and then recycle this back into the logistics (and costs) of trafficking victims from target locations with economically vulnerable populations.

The use of bitcoin to fund trafficking into the U.S. is, as we saw earlier, something that the U.S. Department of Justice is already aware of. Data gathered in the U.S. for this project corroborated this, suggesting that people trafficking routes from Mexico and the Caribbean into the south of the U.S. are often funded by online activities of the gangs responsible for this – for example, from gambling.

Even a brief scrutiny of items available on online markets emphasise how closely cybercriminal activities can be related to other kinds of criminal activity. For example, the takedown of AlphaBay – one of the largest such markets – revealed that, in addition to over 250,000 listings for illegal drugs, there were also listings for toxic chemicals, firearms, counterfeit goods, malware and over 100,000 listings for stolen and fraudulent identification documents and access devices (Europol, 2017).

"Islamic terrorism already has access to its own ready-made funding and laundering service, in the form of the *Hawala* money transfer mechanism."

Perhaps one of the most serious instances of reinvesting cybercrime revenues into further crime centres upon the increasingly strong relationships between the misuse of information technology and the promotion of terrorism. Islamic terrorism already has access to its own ready-made funding and

laundering service, in the form of the *Hawala* money transfer mechanism.

This informal financial network does not require any technical infrastructure and has been found to be used in known terrorist centres of operation such as northern Nigeria, Yemen and the Horn of Africa. But terrorists have been as equally adept in using more digitally focused laundering methods. In 2016, for example, the online jihadist media unit Ibn Taymiyyah Media Center, situated in the Gaza Strip, attempted to raise funding through social media by requesting donations in bitcoin. Evidence has also emerged of ISIS-affiliated militants in Indonesia conducting transactions with individuals in Syria using bitcoin or PayPal (Maxey, 2017). Bitcoin has also been found to have been used by ISIS for funding the movement of personnel and resources into Syria, in order to evade detection (Irwin and Milad, 2016).

"There have even been cases where cybercrimes have been committed specifically in order to generate revenues for terrorism."

Cybercriminal infrastructures for laundering cash have also offered more direct support for terrorist activities. For example, contributors to the al-Fallujah forum – a notorious extremist social media site – indicated there was a steady flow of funding from cybercrime activities and advice was offered on how to evade authorities who might be monitoring electronic payment services (Jacobsen, 2009).

The misuse of social media for terrorist propaganda has also proved a useful way of acquiring financial support. At its height,

ISIS was sending out almost 40,000 tweets per day and more than 1,000 accounts purportedly linked to the terror group have now been suspended by Twitter (Telegraph, 2014).

There have even been cases where cybercrimes have been committed specifically in order to generate revenues for terrorism. Though much of the data on this is necessarily covert and unavailable for public scrutiny, we know of at least some cases of this kind. For example, the British-born follower of Al Qaeda, Younis Tsouli (better known by his online alias "Irhabi 007"), provided technical assistance to the terror group in relation to uploading videos. Tsouli quickly realised that his technical skills could also be used to commit cybercrimes, which would provide new funding sources for the organisation.

Together with his accomplice, Tariq al-Daour, Tsouli began to acquire stolen credit card numbers through transactions on online forums such as Cardplanet. Tsouli succeeded in gathering over 37,000 separate card data files by the time he was arrested – data he used to generate more than $3.5 million in revenues (Jacobsen, 2009). Tsouli also made ample use of the resources offered by The Web of Profit to launder this money through gambling websites, like absolutepoker.com and paradisepoker.com.

Chapter 6: Implications and Recommendations

In revisiting the cybercrime problem through the lens of the revenues it generates and how these are moved around and disposed, the scale and complexity of the cybercrime landscape has become apparent.

In particular, key takeaways include:

- The old idea that cybercrime is like a business needs to be replaced with a new metaphor that better captures its internal complexities; that is, that cybercrime now has its own economy – a literal "web of profit" that not only mirrors its legitimate counterpart, but that both feeds off it and feeds into it.
- Long term solutions will require more sensitivity to the *systemic* aspects of cybercrime – in particular, the economy that supports it. Cybercrime needs to be approached more holistically, as a dynamically evolving field composed of multiple actors and interdependencies, some of which may

not always appear immediately relevant to a particular breach or security incident.

- Economic reasons for engaging in cybercrime now constitute one of its primary motivations. Re-envisioning cyberattacks on systems in terms of economic gain, rather than damage or data acquisition, may help generate new kinds of solutions. For example, it may stimulate better understanding of what kind of data on the black market is considered valuable and where resources should be directed.
- Cybercrime now offers a relatively easy, low start-up cost way of generating revenues – revenues that often far exceed those that can be made from traditional crimes, like armed robbery. In many cases, its revenues are also more significant than those which can be made from legitimate business.
- Focusing upon specific kinds of cybercrimes and the way they are committed will only be effective up to a certain point. Without a more holistic overview, one where the dynamic and interconnected nature of the cybercrime economy is appreciated, understanding of the problem is only ever likely to be partial or incomplete.
- In turn, unless the close interrelations between the cybereconomy and the legitimate economy are taken into consideration, there is a danger that clinging to traditional models of criminality – or, indeed, cyber-criminality – will impede more effective ways of conceptualising responses.
- Integral to all of this is the need for better understanding of how platforms – legal, or illegal – enable and support cybercriminal behaviours. One of the most prominent

examples of the shift towards platform criminality that this research has uncovered, is the explosion of illicit or illegal online markets. These now constitute the single biggest form of revenue generation open to cybercriminals. Cybersecurity professionals will need to be far more proactive in finding tools for infiltrating, undermining and blocking activities across them.

- Theft of corporate secrets also now represents a significant revenue-generating stream within cybercrime. This is both an internally and externally generated problem, but its current form goes beyond traditional constructions of insider threats or malicious actors. More sensitive policy and software solutions will be required to manage this than simplistic forms of surveillance and monitoring, which are merely likely to increase employee alienation and thereby worsen the problem.
- The near exponential rises in cybercrime revenues are providing a pool of resources for sponsoring and supporting further crimes. Some of these now extend beyond cybercrime itself, into more serious offending such as trafficking or terrorism. It is essential to find technical or policing approaches to stem the cybercrime revenues that are being re-invested into crime.
- The reality that nation states, corporations and other legitimate actors now play a key role in revenue generation, laundering and revenue disposal within the cybercrime economy must be properly acknowledged. In The Web of Profit, there are few safe havens. Whilst this might seem like an issue that police or cybersecurity professionals have little control over, better tools for measuring trust, or a greater

readiness to aggressively disrupt and respond to threats are amongst a range of options for better management of this problem.

For those with a more front-end role in tackling the cybercrime problem – most obviously those in the cybersecurity and law enforcement spheres – there are more immediately practical implications of this research that supplement the conceptual issues it has raised. Some of the more obvious of these are listed below:

Recommendations for Law Enforcement

Police need to move beyond a mindset that treats cybercrime solely in terms of crime control and crime prevention approaches and move towards more agile approaches that can keep pace with the rapid shifts within the cybercrime economy. Police intelligence gathering and policing interventions need to focus more directly on the economic structures of cyber-criminality and how these contribute to perpetrator motivations and methods. For example, it will be useful for police and court records to keep clearer accounts of how suspects or convicted cybercriminals generated revenues and what they did with them.

Traditional market reduction approaches to crime control will need to be tailored more towards the hyperconnected marketplaces on which cyber-criminality depends and new methods for disrupting or diminishing economic gain developed. In particular, more intelligence gathering needs to be centred round how *flows* of revenues – data-driven or otherwise – move through the cybercrime economy. Key to this will be the acquisition of more sophisticated analytic tools for

identifying primary revenue points and the use of new techniques, like agent-based modelling, which enable real time simulations of revenue generation and ways in which this can be disrupted.

Predictive software and the use of automated intelligence is likely to contribute to this goal. Such tools may also be helpful in targeting new ways in which criminals use digital means to engage in the traditional cash out process – that is, to spend laundered revenue or convert it into useable forms of value.

Beyond the use of policing technology, better resourced, more specialist teams with a range of cyber-specific policing and financial skills are required. Such teams will need to quickly develop expertise around the criminal use of cryptocurrencies, digital payment systems and other elements of the cybercrime economy. They will also require tools that can help them to deconstruct malware and conduct kill chain analysis in order to identify the source of malware and other variants.

Policing agencies will also need to work more closely with platform providers to target their misuse and to support them in reducing the criminal opportunities they enable.

Recommendations for Cybersecurity Professionals

The cybersecurity industry will need to move beyond simplistic firefighting or responsive measures to cybercrime and focus more clearly on how to respond to the cybercrime economy as a whole.

Greater awareness is required on the part of cybersecurity professionals of the need to work more closely with financial agencies and with the police to identify strategic nodes and

weak points within The Web of Profit where interventions can be most profitably directed.

As part of this, it must be recognised that data and data protection is now about far more than privacy. As one of the key raw materials for generating wealth in both the legitimate and cybercrime economies, data needs to be handled more like traditional currencies and protected with more specific safeguards, such as restrictions on exchange and better regulation of the money supply.

New kinds of software tools are required for uncovering how cybercriminals are using digital technologies for hiding and laundering revenues. One example would be virtualisation tools that can generate safe havens, isolated from the internet, where illicit revenue-generating activity can be diverted and neutralised. Another would be more sophisticated scanning tools capable of better tracking and locating items of value across the net – in particular, personal data.

Yet ultimately, the industry should focus more on *prevention* and ensuring that data is protected, to disrupt cybercrime supply chains.

Recommendations for Academic and Other Researchers

Cybercrime researchers need urgently to gather better data around the three key stages of cybercrime revenue generation identified above. More comprehensive counting of cybercrime revenues, which can refine and develop understanding of the baseline revenue estimates provided in this report, will also be needed.

One important way in which data here can be enhanced, is by widening the range of revenue-generating cybercrime categories included, or by including variables within each category for counting. For example, by acquiring robust estimates of revenues for more kinds of data being traded, such as medical records

Enhanced revenue data will need to be linked to the development of new theoretical models around cybercrime, models where economic motivations play a more prominent causal-explanatory role.

Appendix: Methodology

Research for this report aimed to track and to model the following three factors:

1. Typical origins, volumes and varieties of cybercrime revenues.
2. Routings for these revenues and modes of concealing them from law enforcement.
3. Destinations and utilisations of revenues.

Research was conducted utilising a mixed methods approach which deployed a combination of two key measurement tools:

- Interview and observation data drawn from a sample (n=100) of convicted or currently active cybercriminals. Data gathered here was broken down as follows:
  - Interviews conducted between June 2017-November 2017 with convicted cybercriminals (n=25).
  - Interviews conducted online between October 2017-January 2018 with individuals currently engaged in cybercrime-related activities (n=25).

- Conversation log data and observations across a range of clear/open web or dark web forums collected between August 2017-December 2017 (n=50).

- Interviews and consultations with over 50 expert respondents drawn from policing, financial, cybersecurity and academic spheres. Respondents were selected using a mixture of direct or personal contact and snowball sampling approaches.
- Interview material and observations utilised a semi-structured approach, utilising questions and observational criteria centred upon five key lines of inquiry;
  - *Cybercrime type* – with special attention paid to individuals engaged in one of the selected areas detailed above
  - *Typical revenues* – (if any) received from the crime
  - *Methods* – how revenues were acquired
  - *Movement* – how and if revenues were laundered
  - *Disposal* – how revenues were spent

These primary data sources were supplemented by an extensive range of secondary materials including peer-reviewed academic research; intelligence reports; security and financial databases; media reports; and a range of dark web material and other indicative sources, such as forums and chatrooms.

Note on Revenue Calculations

Any attempt to estimate cybercrime revenues or cost is almost bound to face significant data gaps, or to be superseded by better, more accurate estimates. Whilst this should constitute

a reason for healthy scepticism about such exercises, it does not mean that it is completely impossible to derive estimates. Nor that they are pointless. Whilst the drawbacks and flaws of attempting to cost any aspect of cybercrime are well-known to anyone who researches the field, it is certainly useful to set out benchmarks wherever possible. If the flaws can be kept to a minimum, such benchmarks can provide a useful starting point for future researchers seeking to develop and refine thinking here. At the very least then, they have the advantage of beginning a dialogue.

It is in this spirit that the attempts in this research to derive revenues illustrate the current state of play within the cybercrime economy were initiated. By erring on the side of caution, by making projections from a small, rather than large number of revenue categories and by opting for lower, rather than higher points on the estimate range, the aim was to understand whether the assumption that cybercrime is a lucrative form of offending has any basis in what is actually happening within the cybercrime economy. The surprisingly high figures that were eventually derived certainly suggest that we need to think more seriously about the attractions and how these might be tackled. For even if the figure for total revenues from cybercrime is only accurate up to a point, the fact that it is a deliberately conservative one means that its inaccuracies at least involve only underestimates, rather than overestimates.

A figure of around $1.5 trillion was derived as a conservative estimate of the annual global revenues being derived from cybercrime. The figure was derived by summing revenues obtained from five key categories of revenue-generating cybercrime:

Crime	Annual Revenues*
Illicit, illegal online markets	$860 billion
Trade secret, IP theft	$500 billion
Data trading**	$160 billion
Crimeware, CaaS (Cybercrime-as-a-Service)	$1.6 billion
Ransomware***	$1 billion

Table 9: Annual Cybercrime Revenue Estimates

Illicit Online Market Revenues – $860 billion

This was derived by summing revenues from three well-evidenced types of illicit online markets:

- *Illegal online drug sales* – ~$180 million per annum (cf. Kruithof et al, 2016). Probably a very low estimate given the known $1 billion of profits made from the Silk Road marketplace over two years. For this reason, the higher end estimate was adopted.
- *Illicit pharmaceutical sales* – ~$431 billion per annum (Scott, 2016). This research found that illicit online pharmacies were regularly selling goods where there was counterfeiting, substandard formulation, contamination, fakery, and active ingredient substitution.
- *Counterfeit goods sold online* – ~$460 billion per annum. Worldwide trade in counterfeit goods is estimated at over $17.9 trillion (OECD, 2016) with up to $460 billion of this traded mostly online (Klara, 2017).

Total = $1.071 trillion+

Both of the sources for revenues from counterfeit goods and pharmaceutical suggested that these revenues were mostly derived from items sold online, but the precise volume was left a little unclear.

To estimate, it was therefore assumed that up to 20% of the above total involved goods not sold online, or was lost to the costs of setting up such an operation. Costs are fairly minimal when creating an online marketplace, but as with all the estimates here, the decision was taken to go for the lower end of the scale. Given the 20% lost to offline sales or to costs, a figure of **$860 billion** was derived for online sales.

Trade Secret/IP theft – $500 billion

This figure was derived from two sources:

- *Trade secrets and corporate IP stolen* – ~$200 billion per annum. Recent estimates suggest that the annual cost of economic espionage to the world economy is more than $445 billion — or almost 1% of global income (Center for Strategic and International Studies, 2014). The nature of the perpetrators here (often States and other larger actors) mean than it is difficult to determine profits/revenues as such. But even assuming the value of the asset declines by 50% as a result of the costs of acquiring it and other losses in the transfer, then the profits still stand at around $200 billion.
- *Pirated music/film* – ~$300 billion per annum (IPC, 2013). This figure is for the U.S. – the global figure is likely to be much higher.

Total = $500 billion

This was one of the most difficult calculations given the incomplete data sources, the inconsistency of many prices across different sources and the volatility of prices. Attempting to evaluate revenues for every kind of revenue here, and in any kind of plausible way is almost impossible so to compensate and arrive at a minimal estimate of revenues – just four activities were selected:

1. Stolen card data losses (use-value of the cards).
2. Trading in stolen cards.
3. Trading in bank or payment system data.
4. Trading in login data to websites etc.

We know that up to four billion data records were stolen in 2016 (RBS, 2016) and this figure has remained at roughly between two to four billion to 2017. We don't however know the data churn here – that is, how many of the records stolen actually make it onto online markets. However, in the case of the more than one billion Yahoo! records stolen from 2012, it seems that most ultimately were offered for sale in some form. Based on this paradigmatic data breach, it would therefore appear to be a reasonable assumption that a large portion of stolen data records are ultimately made available for sale. But assuming a more modest turnover of around 75% of stolen records ever becoming available for illicit trading, a baseline figure of around three billion stolen data records traded annually can be deduced.

If this three billion figure is correlated against data for sale across more than 20 sites that were researched, the following breakdown of differing data types for sale emerges:

- *Stolen card data* – around 50% of what was found (i.e. around 1.5 billion available for sale).
- *Banking or payment system login data* – around 20% of what was found (i.e. around 600 million records available for sale).
- *Login credentials for Netflix, apps and other* – around 30% of what was found (around 900 million records for sale).

It's then possible to calculate some revenues for these using prices obtained from various studies (e.g. McAfee, 2015) and other prices found on five dark web sites that were sampled. Using midpoint prices in available scales the following emerges:

- **Credit card data** is worth approximately $10 each (average sale value per record in 2016-2017). Research found 1.5 billion available at $10, for a total of **$15 billion**.
- **Banking or payment system data** is worth approximately $190 each (average sale value per record in 2016-2017). Research found 600 million records available at $190, for a total of **$114 billion**.
- **Login credentials** are worth approximately $0.55 each (average sale value per record in 2016-2017). Research found 900 million records available at $0.55, for a total of **$495 million**.
- **Use of stolen cards** have an estimated loss (revenues) during 2016-2017 of **$30 billion**.

Total = $160 billion

Revenues are actually likely to be much higher than this if higher prices were taken into account, or other types of records such as loyalty points, medical records, social security numbers, credit ratings and so on were also included.

Crimeware (CaaS) – $1.6 billion+

Similar difficulties as those for calculating data trading revenue confront any researcher trying to make sense of the revenues to be had from the multifarious commodities and services available on crimeware or Cybercrime-as-a-Service platforms. A similar, minimalist approach was used, which based the estimate on just three types of revenue-generating activities: DDoS/botnet hire; malware purchase or hire; and hiring basic hacking services. Evidence for pricing was drawn from a sample of five online dark web fora accessed between July 2017-January 2018 and combined with available published research data:

- *DDoS attack/botnet hire* – ~$13 million per annum. This estimate was based on two factors:

    1) Hiring a DDoS/botnet, which came out at an average cost of around $200 per day depending upon how long the attack was and what its strength might be. Some sources (e.g. Ablon et al, 2014) found DDoS hire could cost as much as $1,000.

    2) These costs can then be correlated against current estimates of an average of 6.5 million DDoS attacks over the year (Khalimonenko & Kupreev, 2017). However, allowances must be made for the fact that the same botnet might be deployed more than once and of

course that not every DDoS attack will involve one that has been hired. Assuming then that only 1% of attacks involve a hired DDoS/botnet, a revenue total of **$13 million** can be derived (i.e. 65,000 attacks × $200 per hire).

- *Malware hire* – ~$11 million per annum. This estimate was based upon the combined value of purchasing just two varieties of malware:

    1) *Exploits* – the cost of which varied significantly across the data-sources studied and sites sampled. On the now-discontinued RealDeal site, prices for more higher demand exploits, especially those involving Apple systems, were very high – around $17,000 for an Apple Cloud exploit and up to $250,000 for iOS exploits. Recent research (Ablon et al, 2017) found that the Blackhole exploit kit was being sold for around $1,500. Other data (e.g. Secureworks, 2016), which has been corroborated by findings on the sites sampled for this research, found exploits could also be had for as little as $100. Using this lower, $100 figure for exploits and correlating this against just 1% of the estimated eight million exploit kit attacks in 2016 (Escueta, 2017), it was possible to derive revenues of **$8 million** for the sale of exploits (i.e. 80,000 × $100).

    2) *Remote Access Trojans (RATs)* – this kind of malware could be acquired for as little as $10 from the sites examined and in various published sources. We know that 23% of 127 million malware samples in 2016 involved Trojans (AV-Test, 2017), which amounts to around 29.21 million cases. If we again assume that just

1% of these involve RATs that were purchased, this gives a rounded-up figure of around **$3 million** (i.e. 292,100 × $10).

- *Hire-a-Hacker Services* – ~$1.6 billion **per annum**. This estimate was based on two factors**:**

  1) As with the other costs for crime services listed above, the price of hiring hacking services varied quite widely. One source (Weissman, 2015) listed the price of attacking a website at $2,000, whilst another found that hiring someone to hack and steal data could cost a lower rate of around $350 (Secureworks, 2016). Small jobs – such as hacking an email account – were costed at an average of around $200 according to sources examined and across the sites sampled.

  2) There were four billion social media users in 2017 and Google has estimated that around 20% of social media accounts are hacked per year. This comes to around 80 million hacks. Given both that hacking of social media and hacking-for-hire appear to be more prevalent than the above CaaS indicators we can assume that a slightly more generous (though still very conservative) 10% of these hacks involved a hired service. This gives us a figure of **$1.6 billion** in hacking revenues (i.e. 8 million × $200). Though strikingly high, this is presumably still an underestimate given that hacker-for-hire involves a far greater range of targets than social media accounts alone.

Total = $1.6 billion

Note that many more services than these are advertised on CaaS sites. For example: DDoS cloud attacks; phishing email sites and campaigns; access to Gmail; loyalty points from hotels, airlines etc.; changing essay grades; deleting records (e.g. driving licence points or criminal records); and Amazon reviews. Given that no revenues from these have been included, it is again likely that revenues from crimeware are likely to be much higher than the total given here.

Cyber-Laundering – up to $200 billion

At least two sources triangulate to this figure. Firstly, Europol has estimated that cryptocurrencies constitute around 4% of laundered money in Europe alone at present. Correlated against the UNODC figure for total global laundering of up to $2 trillion, this would mean a baseline figure for laundered cybercrime revenues of at least $80 billion. But there are of course many more ways in which cyber revenues are laundered than by the use of cryptocurrencies.

We know, for example, of mule and reshipping operations that have succeeded in laundering up to $2 billion. Just 30 such operations globally would mean around $60 billion in mule laundering. Factoring in other known varieties of laundering to have involved cybercriminals, such as the use of legitimate banks or online gambling, there is at least another $60 billion that could be included – and indubitably far more. This gives us a figure of up to $200 billion in cyber-laundering revenues (i.e. $60 billion + $80 billion + $60 billion = $200 billion).

Total = up to $200 billion

Index

Bibliography

Ablon, L., Libicki, M.C. and Golay, A.A. (2014). *Markets for Cybercrime Tools and Stolen Data*. RAND.

Anand, P. (2015). *'18 most popular things fraudsters buy with your credit card'* [online]. Market Watch. Available at: https://www.marketwatch.com/story/18-most-popular-things-fraudsters-buy-with-your-credit-card-2015-11-24

Anderson R., Barton, C., Böhme, R., Clayton, R., van Eeten, M.J.G., Levi, M., Moore, T. and Savage, S. (2012). *Measuring the Cost of Cybercrime*. Paper presented at the Weis 202 Workshop on the Economics of Information Security Berlin, Germany, 25-26th June 2012.

Apps, P. and Finkle, J. (2014). *Suspected Russian Spyware Turla Targets Europe*, *United States* [online]. Reuters. Available at: https://www.reuters.com/article/us-russia-cyberespionage-insight/suspected-russian-spyware-turla-targets-europe-united-states-idUSBREA260YI20140307

AV-Test (2017). *Security Report 2016/7* [online]. Accessed at: https://www.av-test.org/fileadmin/pdf/security_report/AV-TEST_Security_Report_2016-2017.pdf

Barth, B. (2016). *Snack attack: A crimeware-as-a-service menu for wannabe hackers* [online]. SC Media. Accessed at: https://www.scmagazine.com/snack-attack-a-crimeware-as-a-service-menu-for-wannabe-hackers/article/527865/

BBC (2014). *Snapchat hack affects 4.6 million users* [online]. BBC News. Accessed at: http://www.bbc.co.uk/news/technology-25572661

BBC (2015). *Fake luxury goods online sites closed by police* [online]. BBC News. Accessed at: http://www.bbc.co.uk/news/technology-31454822

Beaming (2017). *Cyberthreat Report 2017:Attacks on UK businesses increase to 231,028 each* [online]. Beaming. Accessed at: https://www.beaming.co.uk/cyber-reports/cyber-attacks-uk-businesses-increase-231028-2017/

Bengineer (2015). *How to Steal Form Data from Your Fake Website* [online]. Null Byte. Accessed at: https://null-byte.wonderhowto.com/how-to/steal-form-data-from-your-fake-website-0164112/

Benyawa, L. (2016). *Agency says 3000 cyber-crime cases reported in Kenya monthly* [online]. Standard Digital. Accessed at: https://www.standardmedia.co.ke/business/article/2000204352/agency-says-3000-cyber-crime-cases-reported-in-kenya-monthly

Berson, S (2017). *Manafort rented out illegal AirBnb, indictment says. So did his daughter, lawsuit claimed* [online]. Miami Herald. Accessed at: http://www.miamiherald.com/news/nation-world/national/article181676271.html

Bowers, S. (2016) *MPs poised to investigate VAT fraud on Amazon and eBay* [online]. The Guardian. Accessed at:

https://www.theguardian.com/business/2016/dec/21/mps-vat-fraud-amazon-ebay-public-accounts-committee

Bouchard, M. and Wilkins, C. (2010). *Illegal Markets and the Economics of Organised Crime*. Routledge.

Brown, J. (2016). *The average hacker makes less than $30,000 a year* [online]. The Week. Accessed at: http://theweek.com/articles/604630/average-hacker-makes-less-than-30000-year

Button, M. and Cross, C. (2017). *Cyber Frauds, Scams and Their Victims*. London: Taylor And Francis.

Carlisle, D. (2017). *Virtual Currencies and Financial Crime: Challenges and Opportunities*. RUSI.

CCFS (2016). *Annual Fraud Indicator*. Centre for Counter Fraud Studies, University of Portsmouth.

Chaffey, D. (2017). *Forecast growth in percentage of online retail / Ecommerce sales* [online]. Smart Insights. Accessed at: https://www.smartinsights.com/digital-marketing-strategy/online-retail-sales-growth/

Cosgrave, J. (2014). *Online gambling: The new home for money launderers?* [online]. CNBC. Accessed at: https://www.cnbc.com/2014/04/25/online-gambling-the-new-home-for-money-launderers.html

Cox, J. (2017). *Inside Airbnb's Russian Money-Laundering Problem* [online]. The Daily Beast. Accessed at: https://www.thedailybeast.com/inside-airbnbs-russian-money-laundering-problem

CSIS (2014). *Estimating the Global Cost of Cybercrime*. Centre for Strategic and International Studies/McAfee

Cybersecurity Ventures 2017 *Annual Cybercrime Report.*

Davies, R. (2018). *Five UK online casinos may lose licence over money-laundering fears* [online]. The Guardian. Accessed at: https://www.theguardian.com/society/2018/jan/05/five-of-uk-online-casinos-may-lose-licence-over-money-laundering-fears

DCA (2014). *Good Money Gone Bad: Digital Thieves and the Hijacking of the Online Ad Business.* Digital Citizens Alliance

Detica (2011). *The Cost of Cybercrime*. Detica and UK Cabinet Office.

Dreyer, P., Jones, T., Klima, K., Oberholtzer, J., Strong, A., Welburn, W. and Winkelman, Z. (2018). *Estimating the Global Cost of Cyber Risk*. RAND.

Dubourg, R. and Prichard, A. (2008). *Organised crime: revenues, economic and social costs, and criminal assets available for seizure*. UK Home Office.

Economist (2016). *Buying drugs online: shedding light on the dark web* [online]. The Economist. Accessed at: https://www.economist.com/news/international/21702176-drug-trade-moving-street-online-cryptomarkets-forced-compete

Escueta, G. (2017). *Tracking the Decline of Top Exploit Kits* [online]. Trendlabs Security Intelligence Blog. Accessed at: https://blog.trendmicro.com/trendlabs-security-intelligence/tracking-decline-top-exploit-kits/

Eurostat (2017). *E-commerce statistics for individuals.* Data extracted from 2017 Survey on ICT usage in households and by individuals.

Europol (2016). *178 arrests in successful hit against money muling* [online]. Europol press release. Accessed at: https://www.europol.europa.eu/newsroom/news/178-arrests-in-successful-hit-against-money-muling

Europol (2017). *How Illegal Drugs Sustain Organised Crime in Europe* [online]. Europol Business Fundamentals Report. Accessed at: https://www.europol.europa.eu/publications-documents/how-illegal-drugs-sustain-organised-crime-in-eu

Fahmy, D. (2010). *Credit Card Crooks Like to Shop at Best Buy, Target, Amazon* [online]. ABC News. Accessed at: http://abcnews.go.com/Business/credit-card-theft-crooks-shop-best-buy-target/story?id=9931006

Fossbytes (2017). *How Much Money Torrent Sites Like The Pirate Bay And KickassTorrents Make?* [online]. Fossbytes. Accessed at: https://fossbytes.com/how-much-money-torrent-site-make-pirate-bay-kickass/

Fox-Brewster, T. (2017). *Google Warns Ransomware Boom Scored Crooks $2 Million A Month* [online]. Forbes. Accessed at: https://www.forbes.com/sites/thomasbrewster/2017/07/25/google-ransomware-multi-million-dollar-business-with-locky-and-cerber/#51fd09266caf

Freeman, R. and Holzer, H. (1986). *The Black Youth Employment Crisi*s. University of Chicago Press.

GFI (2017). *Transnational Crime and the Developing World*. Global Financial Integrity.

Goldfeder, S., Kalodner, H., Reisman, D. and Narayanan, A. (2017). *When the cookie meets the blockchain: Privacy risks of web*

payments via cryptocurrencies [online]. Cornell University. Accessed at: https://arxiv.org/abs/1708.04748

Grabosky, P., Smith, R.G. and Dempsey, G. (2002). *Electronic Theft: UnlawfulAcquisition in Cyberspace*. Cambridge: Cambridge University Press.

Greenberg, A. (2013). *FBI Says It's Seized $28.5 Million In Bitcoins From Ross Ulbricht* [online]. Forbes. Accessed at: https://www.forbes.com/sites/andygreenberg/2013/10/25/fbi-says-its-seized-20-million-in-bitcoins-from-ross-ulbricht-alleged-owner-of-silk-road/#76df4feb2765

GSMA (2017). *State of the Industry Report on Mobile Money* [online]. Accessed at: https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2017/03/GSMA_State-of-the-Industry-Report-on-Mobile-Money_2016.pdf

Guardian (2016). *Ten arrested in Netherlands over bitcoin money-laundering allegations* [online]. The Guardian. Accessed at: https://www.theguardian.com/technology/2016/jan/20/bitcoin-netherlands-arrests-cars-cash-ecstasy

Hao, S., Borgolte, K., Nikiforakis, N., Stringhini, G., Egele, M., Eubanks, M., Krebs, B. and Vigna, G. (2015) *Drops for Stuff, An Analysis of Reshipping Mule Scams*. ACM Conference on Computer and Communications Security.

Harding, L., Hopkins, N. and Barr, C. (2017). *British banks handled vast sums of laundered Russian money* [online]. The Guardian. Accessed at: https://www.theguardian.com/world/2017/mar/20/british-banks-handled-vast-sums-of-laundered-russian-money

Holt, T., Smirnova, O. and Chua.Y. (2016). *Exploring and Estimating the Revenues and Profits of Participants in Stolen Data Markets*. Deviant Behavior.

Hubbs, R. (2014). *Shell games: Investigating shell companies and understanding their roles in international fraud.* Fraud Magazine, July/August.

ICE (2010). *Mass marketing Fraud, A Threat Assessment*. International Mass Marketing Fraud Working Group, US Immigration and Customs Enforcement.

IOCTA (2017). *Internet Organised Crime Threat Assessment 2017*. Europol.

IPC (2013). *Report on the Theft of American Intellectual Property.*

Irwin, A. and Milad, G. (2016). *The use of crypto-currencies in funding violent jihad*. Journal of Money Laundering Control, 19 4, pp.407-425.

Isaza, A. (2015). Fake Japanese E-Commerce Sites Used for E-commerce [online]. ISBuzz News. Accessed at: https://www.informationsecuritybuzz.com/articles/fake-japanese-e-commerce-sites-used-for-stealing-credit-card-information/

Jacobsen, M. (2009) *Terrorist Financing on the Internet*. CTC Sentinel, June, 2,6.

John (2017). *Corporate Bankers Stealing Own Company Data to Sell on Darknet* [online]. Darknetmarkets.co. Accessed at: https://darknetmarkets.co/corporate-bankers-stealing-own-company-data-to-sell-on-darknet/

Johnson, L. (2017). *Crime-as-a-Service Could Be the Next Big Threat to Your Business* [online]. Entrepreneur. Accessed at: https://www.entrepreneur.com/article/298727

Khalimonenko, A. and Kupreev, O. (2017). *DDos Attacks in Q1 2017* [online]. Securelist. Accessed at: https://securelist.com/ddos-attacks-in-q1-2017/78285/

Khan, I. (2016). *The virtual future of money laundering*. Fraud Magazine, June.

Klara, R. (2017). *Counterfeit Goods Are a $460 Billion Industry, and Most Are Bought and Sold Online*. Adweek. Accessed at: http://www.adweek.com/brand-marketing/counterfeit-goods-are-a-460-billion-industry-and-most-are-bought-and-sold-online/

Krebs, B. (2013). *Crimeware Author Funds Exploit Buying Spree* [online]. Krebs on Security. Accessed at: https://krebsonsecurity.com/2013/01/crimeware-author-funds-exploit-buying-spree/

Krehel, O. (2016). *The rise of LinkedIn fraud* [online]. CSO Online. Accessed at: https://www.csoonline.com/article/3036072/social-networking/the-rise-of-linkedin-fraud.html

Kruisbergen, E., Kleemans, E. and Kouwenberg, R. (2014). *Profitability, Power, or Proximity? Organised Crime Offenders Investing Their Money in Legal Economy*. Eur J Crim Policy Res 21:237–256.

Kruithof, K., Dujso, E. Décary-Hetu, D. and Aldridge, J. (2016). *Internet-facilitated drugs trade*. RAND.

Kuchler, H. (2014). *Cyber criminals eye financial markets for a better return on investment* [online]. Financial Times. Accessed at:

https://www.ft.com/content/2a11ee92-3cbc-11e4-871d-00144feabdc0

Lewis, P. and Hilder, P. (2018). *Leaked: Cambridge Analytica's Blueprint for Trump Victory* [online]. The Guardian. Accessed at: https://www.theguardian.com/uk-news/2018/mar/23/leaked-cambridge-analyticas-blueprint-for-trump-victory

Maxey, L. (2017). *Terror Finance in the Age of Bitcoin* [online]. The Cipher Brief. Accessed at: https://www.thecipherbrief.com/article/tech/terror-finance-age-bitcoin

Machalinksi, A. (2017). *Bitcoin and the Blockchain Are Disruptors in Global Real Estate* [online]. Mansion Global. Accessed at: https://www.mansionglobal.com/articles/77889-bitcoin-and-the-blockchain-are-disruptors-in-global-real-estate

Matthews, L. (2018). *Hackers Abuse Google Ad Network To Spread Malware That Mines Cryptocurrency* [online]. Forbes. Accessed at: https://www.forbes.com/sites/leemathews/2018/01/26/hackers-abuse-google-ad-network-to-spread-malware-that-mines-cryptocurrency/#3e933e987866

McAfee (2015). *The Hidden Data Economy.*

McKeon, A. (2017). *A Look Into the Thriving Dark Web Criminal Market* [online]. Recorded Future. Accessed at: https://www.recordedfuture.com/podcast-episode-30/

NBC (2017). *Ransomware: Now a Billion Dollar a Year Crime and Growing* [online]. NBC News. Accessed at: https://www.nbcnews.com/tech/security/ransomware-now-billion-dollar-year-crime-growing-n704646

NCA (2016). *Cybercrime Assessment 2016*. UK National Crime Agency.

Nguyen, H. and Loughran, T. (2017). *On The Reliability And Validity Of Self-Reported Illegal Earnings: Implications For The Study Of Criminal Achievement*. Criminology, 5, 3, pp. 575–602.

Nilson (2016). *Card Fraud Losses Reach $21.84 Billion*. Nilson Report, Issue 1096.

Norton (2011). *Annual Cybercrime Report.*

OECD (2016). *Trade in Counterfeit and Pirated Goods.*

Paganini, P. (2017). *Western Union agreed to pay $586 Million to settle fraud charges* [online]. Security Affairs. Accessed at: http://securityaffairs.co/wordpress/55573/breaking-news/western-union-settlement.html

Palmer, D. (2017) *Dark web vendors are selling remote access to corporate PCs for as little as $3* [online]. ZDnet. Accessed at: https://www.zdnet.com/article/dark-web-vendors-are-selling-remote-access-to-corporate-pcs-for-as-little-as-3/

Panda (2010). *Western Union Entwined with Cybercrime?* [online]. Panda Security Mediacenter. Accessed at: https://www.pandasecurity.com/mediacenter/malware/western-union-entwined-with-cybercrime/

Perez, S. (2017). *We Heart It says a Data Breach affected over 8 million Accounts* [online]. TechCrunch. Accessed at: https://techcrunch.com/2017/10/16/we-heart-it-says-a-data-breach-affected-over-8-million-accounts-included-emails-and-passwords/

Perlroth, N. (2017). *All 3 billion Yahoo Accounts Were Affected by 2013 Attack* [online]. The New York Times. Accessed at: https://www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html

Ponemon (2015). *Annual Cost of Data Breach Study: Global Analysis*. Ponemon Institute.

Popper, N. (2017). *Bitcoin Exchange Was a Nexus of Crime, Indictment Says* [online]. New York Times. Accessed at: https://www.nytimes.com/2017/07/27/business/dealbook/bitcoin-exchange-was-a-nexus-of-crime-indictment-says.html

Power, M. (2013). *Drugs 2.0*. New York: St Martins Press.

RBS (2016). *Databreach QuickView Report*. Risk Based Security.

Reuter, P. (2005). *Chasing Dirty Money: the Fight Against Money Laundering*. Peterson Institute.

Reuters (2015). *Cybercrime ring steals up to $1 billion from banks: Kaspersky* [online]. Reuters. Accessed at: https://uk.reuters.com/article/uk-cybersecurity-banks/cybercrime-ring-steals-up-to-1-billion-from-banks-kaspersky-idUKKBN0LJ02L20150215

Richet, J.L. (2013). *Laundering Money Online: a review of cybercriminals' methods*. United Nations Office on Drugs and Crime (UNODC), Tools and Resources for Anti-Corruption Knowledge.

Richards, J.R. (1998) *Transnational Criminal Organizations, Cybercrime, and Money Laundering*. CRC Press.

Robinson, T. and Fanusie, Y. (2017). *Bitcoin Laundering: An Analysis of Illicit Flows into Digital Currency Services*. Center on Sanctions and Illicit Finance.

Scott, G. (2016). *The Very Real Risks Behind the $400 Billion Illegal Online Pharmacy Industry* [online]. Medscape. Accessed at: https://www.medscape.com/viewarticle/873704

Secureworks (2016). *Underground Hacker Marketplace Report.*

Shih, G. (2013). *Facebook admits year-long data breach exposed 6 million users* [online]. Reuters. Accessed at: https://uk.reuters.com/article/net-us-facebook-security/facebook-admits-year-long-data-breach-exposed-6-million-users-idUSBRE95K18Y20130621

Silva, S. (2018) *Criminals hide 'billions' in crypto-cash – Europol* [online]. BBC Accessed at: http://www.bbc.com/news/technology-43025787

Siwek, S. (2007). *The True Cost of Sound Recording Piracy to the U.S. Economy*. Institute for Policy Innovation Report.

Sky (2017). *Banker helped gang launder £16m for cybercriminals* [online]. Sky News. Accessed at: https://news.sky.com/story/banker-helped-gang-launder-16m-for-cybercriminals-11044498

Srnicek, N. (2016) *Platform Capitalism*. London: Wiley.

SOCTA 2017 *Serious and Organised Crime Threat Assessment 2017*, Europol

Southport Local (2014). *Nine arrested in ticket fraud investigation.* Southport Local, 15th May 2014.

Steiner, I. (2017) *Rethinking Returns in Wake of $1.2 million Amazon Fraud*. EcommerceBytes Blog. Accessed at: https://www.ecommercebytes.com/C/blog/blog.pl?/pl/2017/10/1506992808.html

Sulleyman, A. (2017). *Kodi Box Seller Who made £370,000 Given Suspended Prison Sentence* [online]. The Independent. Accessed at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/kodi-box-maiz-limited-daniel-david-brown-llansamlet-suspended-prison-sentence-made-370000-profit-a7821601.html

Szabo, A. (2016) *From the Mob to Mario: How Money Laundering Lives on Through Video Games*, Panopticon. Accessed at: https://www.panopticonlabs.com/from-the-mob-to-mario-how-money-laundering-lives-on-through-video-games/

Szoldra, P. (2016). *Hackers are making $7,500 per month by holding people's data hostage* [online]. Business Insider. Accessed at: http://uk.businessinsider.com/flashpoint-report-ransomware-2016-6?r=US&IR=T

Takahashi, D. 2014 *Only 0.15 percent of mobile gamers account for 50 percent of all in game purchases* [online]. Venturebeat. Accessed at: https://venturebeat.com/2014/02/26/only-0-15-of-mobile-gamers-account-for-50-percent-of-all-in-game-revenue-exclusive/

Teicher, R. (2018). *How Uber Ghost Rides are Linked to Money Laundering* [online]. The Next Web. Accessed at: https://thenextweb.com/contributors/2018/03/18/uber-ghost-rides-linked-online-money-laundering/

Telegraph (2014). *How terrorists are using social media* [online]. The Telegraph. Accessed at:

https://www.telegraph.co.uk/news/worldnews/islamic-state/11207681/How-terrorists-are-using-social-media.html

Trend Micro (2016). *The Cybercriminal Roots of Selling Online Gaming Currency*.

Trend Micro (2017). *Threats to Global Business Survey*.

Trustwave (2015). *Global Security Report*.

UCSD (2017). *UC San Diego and NYU estimate 25 million in ransomware payout.* UC San Diego Press release, July 2017.

UNODC (2011). *Estimating Illicit Financial Flows Resulting from Drug Trafficking and Other Transnational Organised Crimes*. United Nations Office on Drugs and Crime Report, October 2011.

Vidalon, D. (2017). *Airbnb drops controversial payment card in France* [online]. Reuters. Accessed at: https://uk.reuters.com/article/us-airbnb-card/airbnb-drops-controversial-payment-card-in-france-idUKKBN1E616B

Vincent, J. (2013). *Instagram Virus Shows that 'Online Likes' are Worth More than Stolen Credit Cards* [online]. The Independent. Accessed at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/instagram-virus-shows-that-online-likes-are-worth-more-than-stolen-credit-cards-8774997.html

Viscusi, W. (1986). *The Risks and Rewards of Criminal Activity: A Comprehensive Test of Criminal Deterrence*. Journal of Labor Economics, 4 3, 317-40.

Wales Online (2015). *Dealer lived the high life on profits from selling illegal drugs and legal highs online* [online]. Wales Online. Accessed at: https://www.walesonline.co.uk/news/wales-news/dealer-lived-high-life-profits-9385858

Wall, D. (2016). *The theft of ideas as a cybercrime: downloading and changes in the business model of creative arts.* In McGuire, M. and Holt, T. (eds) *The Handbook of Technology Crime & Justice*. Routledge.

Ward, V. and Maidment, J. (2017). *Dealers 'using social media sites to sell drugs to teenagers* [online]. The Telegraph. Accessed at: https://www.telegraph.co.uk/news/2017/12/31/dealers-using-social-media-sites-sell-drugs-teenagers/

Weissman, C. (2017). *9 things you can hire a hacker to do and how much it will (generally) cost* [online]. Business Insider: http://uk.businessinsider.com/9-things-you-can-hire-a-hacker-to-do-and-how-much-it-will-generally-cost-2015-5

Whitty, M. T. (2015). *Mass-marketing fraud: A growing concern*. IEEE Security & Privacy, 13(4).

White, G. (2018). *UK company linked to laundered Bitcoin billions* [online]. The BBC. Accessed at: http://www.bbc.co.uk/news/technology-43291026

Biography
Dr. Michael McGuire

Senior Lecturer, University of Surrey

Dr Michael McGuire is Senior Lecturer in Criminology at the University of Surrey, UK. He has developed an international profile in the study of cybercrime, technology and the justice system and has published widely in these areas.

His first book *Hypercrime: The New Geometry of Harm* (Glasshouse, 2008), was the first to define cybercrime in terms of the concept of hyperconnectedness and was awarded the 2008 British Society of Criminology runners up Book Prize.

His most recent publications, *Technology, Crime & Justice: The Question Concerning Technomia* and the *Handbook of Technology, Crime and Justice* (Routledge, 2012 & 2016) have provided comprehensive overviews of the implication of technology for the justice system.

These complement a range of applied studies of cybercrime, including *Organised Crime in the Digital Age* (2012), one of the first studies of how organised crime has shifted to the internet and *Cybercrime, A Review of the Evidence* for the UK Home Office (2014). He is currently one of the lead investigators for the $1.5m *ACCEPT project (Addressing Cybersecurity and Cybercrime via a co-Evolutionary aPproach to reducing human-relaTed risks)* funded by the UK Engineering and Physical Science council. The project aims to develop a co-evolution based methodology for modelling human factors in cybersecurity.

Research Sponsor
Bromium, Inc.

Our mission is to provide security to people who want to use digital communication to advance society – from the free exchange of ideas to allowing for global commerce to the democratization of information and education. While cybercriminals work to threaten online safety, we remain committed to thwarting their efforts through superior technological innovation.

"If you're serious about security,
you should be talking to Bromium."

Our founders, Ian Pratt and Simon Crosby, originally founded XenSource, which built enterprise-class virtualization products based on the Xen hypervisor. XenSource was acquired by Citrix in 2007. They stayed at Citrix for a while and then came up with an idea that would revolutionize endpoint security: virtualization-based security.

The result is the Bromium Secure Platform that essentially protects endpoints from getting owned – eliminating the need for a patient-zero required by today's detect-to-protect solutions. Several governments have already bet on Bromium to protect their employees around the world.

Application Isolation and Control

To many technology folks, Application Isolation may be a new term when it comes to cybersecurity and endpoint protection. This term has been made popular by the National Security Agency (NSA). It detailed how Application Isolation is the way forward for finally stopping advanced, zero-day, and nation-state malware.

"It has often been said, "the only way to stop malware is to not stop malware". That is exactly what Application Isolation is all about."

Fundamentally, stopping malware by using detection is flawed. This will always be a matter of catch up as the writers of malicious code tend to be one step ahead. The general rule is that a person who writes malware only needs to get it right once, while a person who writes software to stop malware needs to get it right every time. This was made publicly evident with recent malware exploits WannaCry and Petya. Most major detection vendors were vulnerable to this exploit as it was something that had never been seen before. While they were quick to develop a method to stop it, what if you were the unlucky person to get this on Day Zero?

The real problem is detection as a method to stop malware. Fred Cohen is a well-respected computer scientist and the inventor of the words "computer virus". He believed that detection was inferior as "there is no algorithm that can perfectly detect all possible viruses".

It has often been said, "the only way to stop malware is to not stop malware".

That is exactly what Application Isolation is all about.

Untrusted Tasks Are Protected

With Application Isolation, as users perform untrusted tasks that could be ingress points for malware, an isolated environment is created to perform that task seamlessly to the user. If malware is part of that task, it can completely play out in the isolated environment with no access to the protected host operating system. This is the classic "honey pot" scenario that malware believes it is fully running and executing, yet only damaging a disposable environment.

"At no point can the malware escape from the virtual machine."

Bromium is exactly that. Bromium isolation runs each untrusted user task in a hardware-isolated virtual machine transparent to the user. Every time a user opens a tab in a browser, an untrusted Office or PDF document, or runs an untrusted executable, Bromium isolation creates a seamless hardware isolated virtual machine that performs the task for the user. If malware is part of that task, it only resides in that virtual machine thus keeping the protected host operating system safe.

While the hardware isolated virtual machine is performing the untrusted task on behalf of the user, Bromium isolation is using introspection from the outside to look into the virtual machine. This means that we are monitoring the virtual machine and looking for any "abnormal" activity. All this threat intelligence, including the entire malware payload, is then collected and sent back to the Bromium controller for SOC team analysis. The forensic detail is ready for the SOC team to analyse and the attack never touched the user's host computer.

"We take the approach of protect before you detect."

In the walk-through below, you'll see how Bromium uses Application Isolation to protect the users from untrusted documents. You'll see how we use introspection to monitor from the outside looking in the hardware isolated virtual machine. Finally, we use VirusTotal as a method to show why detection fails and why Application Isolation works.

First, we launch a Microsoft Word document that has malware hidden inside of it. Using a utility, Bromium Live View, you can see all the running hardware isolated virtual machines on my endpoint. The Word Doc with the malware is running inside "Micro-VM 0123". However, you will see that the document appears to be running just lie any other Word document from the user perspective.

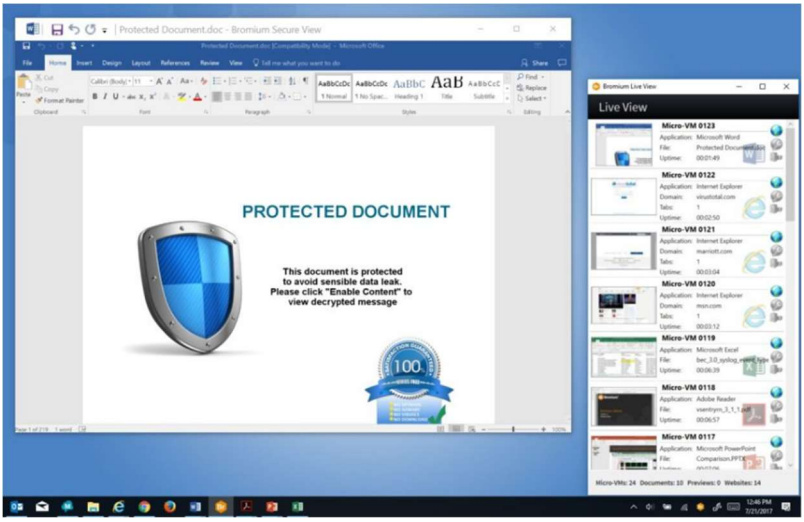


Figure 7: Bromium Live View of Word Document

Once the document is opened in a hardware isolated virtual machine, the malware will start executing its payload. The introspection of Bromium detects that abnormal events are happening; an alert is sent to the user and the SOC team that the document contains malware. However, the malware can only execute in the hardware isolated virtual machine.

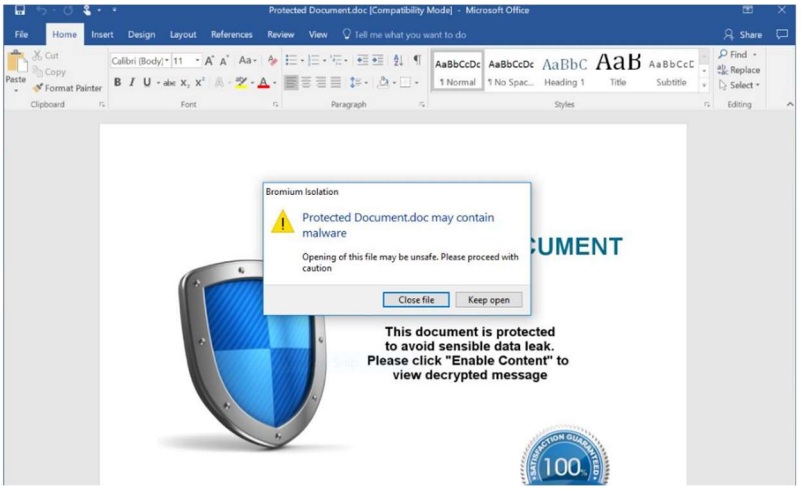


Figure 8: Bromium Warns About Malware

While introspection is running on the virtual machine, all the forensic detail is being sent back to the Bromium Controller server.

The Bromium Controller Provides High Fidelity Alerts

At this point the SOC team can examine the entire kill chain of what the malware did. Because we allow the malware to fully execute, the introspection is in a unique position to see the entire payload and step-by-step of what the malware did. As with most malware, the first step is a "drop and execute". By examining the SHA256 hash of the malware, we can search a public site such as VirusTotal.com to determine what the industry knows about this particular malware.

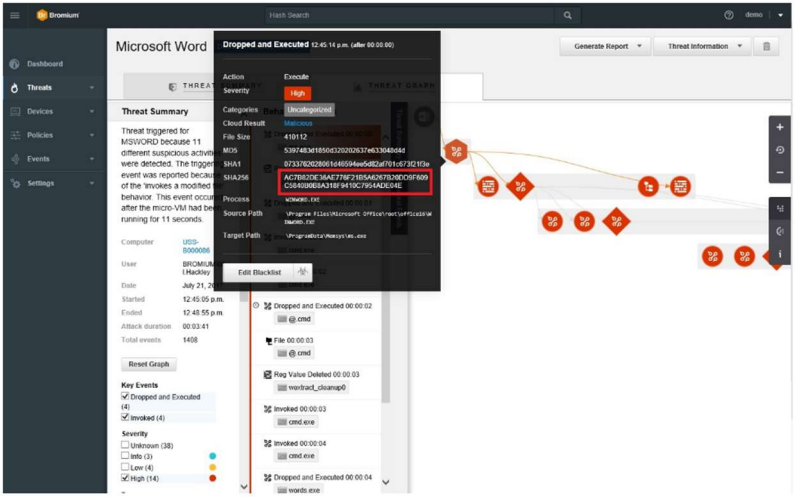


Figure 9: The Bromium Controller Provides Kill Chain Information

VirusTotal.com Explains the Malware

Plugging the SHA256 into the search engine of VirusTotal.com shows the details of this malware. The first thing to notice is that as this is written, the malware payload is already over a year old. The more interesting thing to note as this is written, only 31 of the 57 vendors that report to VirusTotal.com show this file as being malicious. If you are not familiar with how VirusTotal.com reports on this, all the vendors with a "result" in red show the file as malicious.

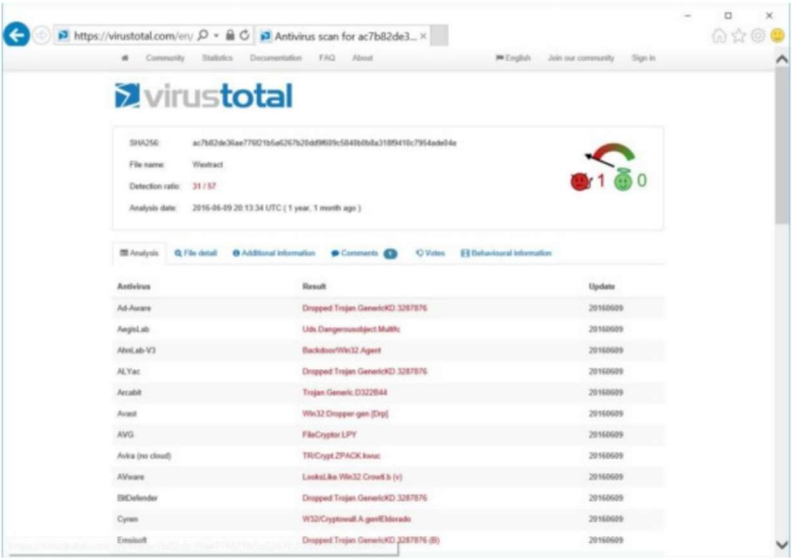


Figure 10: Files in Red Mean This Malware is Still Seen as Malicious

However, scrolling down, the vendors with a "result" of a green check mark do not recognize this file as malicious. That means that if you use any of the vendors with the green check mark, you're not protected from this old malware.

While most of the vendors on the VirusTotal.com list rely on detection, it should be obvious why detection is flawed. It is only as good as the vendor is at updating its signature files. Even "Next-Gen" AV that is not necessarily based on signatures has its drawbacks. Carefully crafted malware will always be one step ahead of any type of detection, even "Next-Gen".

- **Protect email attachments.**

  Employees must open email attachments to do their jobs. Cybercriminals know this and have devised cunning ways to trick users into opening malicious attachments, bypassing layered defenses. Virtualization-based security is the only solution that lets you click with confidence.

  Contain malware. Instantly isolate Outlook and webmail attachments in a secure, disposable micro-VM.

  Protect the host. Malware can't escape from isolation, protecting both online and offline users.

  Stop worrying. No detection is required so even previously unknown threats are completely isolated and contained.

- **Contain phishing attacks.**

  Phishing attacks are constantly evolving and take different forms. They are particularly effective, because employees need to click on links to do their work and social engineering makes phishing links difficult to identify. Virtualization-based security is the only solution that lets you safely open shared links, even if they are malicious.

  Isolate malware. Each browser tab runs in its own secure micro-VM where malicious code is contained and can't access the host.

  Outsmart hackers. Bromium phishing protection also works for malicious links embedded in otherwise benign documents — a common attack tactic designed to bypass conventional detection techniques.

Click with confidence. Stop worrying about clicking on external links and shared URLs and get back to work — no need for restrictive IT security policies.

- **Protect web downloads.**

  Malicious downloads are effective because bad websites are so abundant, short-lived, and contain content that changes frequently to avoid categorization. Virtualization-based security is the only solution that lets you safely download and access documents and executable files.

  Open safely. All document and executable file downloads are automatically and instantaneously opened inside isolated micro-VMs.

  Protect continuously. All files can be safely downloaded and accessed, on any network, and even when disconnected.

  Improve productivity. Eliminate restrictive IT security policies that limit user access to downloaded files and inhibit workflows.

- **Safely access unprotected networks.**

  Modern workers must often go online using unsecured public networks. Requiring remote users to connect to a VPN won't solve the security challenge – VPN offers no protection against sophisticated malware, and users usually don't follow strict security recommendations anyway. Virtualization-based security is the only solution that secures employee access when they use unprotected networks.

  Open any content. All types of files, links, browser windows, images, zip archives, and rich media content are automatically isolated inside a secure micro-VM.

Maintain performance. Native applications run inside micro-VMs—not remote renders—offering a familiar user experience, speed, and performance.

Improve employee productivity. Don't force your users to go through slow, restrictive, and cumbersome security layers. Protect them on any network, with no risk of a breach.

- **Safely visit uncategorized websites.**

  Many websites are now encrypted, but malware still finds a way to get through, outsmarting encryption and skirting layered defenses. Categorization is not much help either – categories are often incorrect, incomplete, or obsolete. Virtualization-based security is the only way to reliably protect users from malware, while allowing them to browse without restrictions.

  Access content from any websites. Bromium assumes that anything could be malicious, and opens each file, tab, or document in a unique, secure container.

  Visit any URL. Your employees will keep visiting uncategorized websites – don't try to stop them, protect them with application isolation.

  Ease the IT burden. Eliminate tedious manual site exception reviews and free up your security administrators.

- **Defense-grade security – when you need full-protection.**

  Bromium application isolation is the last line of defense when other endpoint security solutions fail. Protect your most vulnerable vectors: email file attachments, executables,

email links, and browser downloads. Virtualization-based security is the only solution that stops nation-state and zero-day attacks.

Contain malware. Automatically and instantly isolate tasks and content in a secure, disposable micro-VM.

Protect the host. Malware can't escape from isolation, protecting both online and offline users.

Stop worrying. No detection is required so even previously unknown threats are completely isolated and contained.

If this has piqued your interest, give Bromium a call. It may be time to trust the advice of our friends at the NSA and take a serious look at Application Isolation.