BEHIND THE DARK NET BLACK MIRROR THREATS AGAINST THE ENTERPRISE

The next chapter of *Into The Web of Profit*

By Dr. Michael McGuire,
Senior Lecturer in Criminology,
University of Surrey

CONTENTS

Executive summary

Introduction: Catching smoke – the challenges of navigating the increasingly invisible net

1 The dark net economy – platforms, commodities and profits

- 1.2 The multidimensional risk posed by the dark net to the enterprise – a 3D threat assessment
- 1.3 Tools and services being sold to enable compromises of enterprise networks
  - 1.3.1 Infection/attack tools
  - 1.3.2 Access
  - 1.3.3 Targeting and espionage
  - 1.3.4 Support services
- 1.4 Tools and services being sold to enable financially-motivated compromises
  - 1.4.1 Card credentials
  - 1.4.2 Phishing tools
  - 1.4.3 Refunds and other scams
- 1.5 Tools and services being sold to compromise data
  - 1.5.1 Customer data
  - 1.5.2 Operational data
  - 1.5.3 Financial data
  - 1.5.4 Trade secrets and intellectual property

2 Dark net enablement of traditional crime relating to the enterprise

- 2.1 Insider trading on the dark net
- 2.2 Recruitment and fraud

3 Enterprise and the grey net: quasi-legal uses of the dark net

- 3.1 Competitive intelligence or corporate espionage?
- 3.2 Sharing blacklists

4 The legitimate commercialisation of the dark net by the enterprise

- 4.1 Cybersecurity
- 4.2 Secure communication
- 4.3 Business intelligence
- 4.4 Credit monitoring
- 4.5 Recruitment
- 4.6 Potential risks of engaging in the dark net

5 Closing thoughts

- 5.1 Recommendations for law enforcement
- 5.2 Recommendations for enterprise

Methodology

Bibliography

FOREWORD

GREGORY WEBB,
CEO of Bromium

Working with Dr. McGuire is always a real eye-opener, and his academic research continues to confirm what we've long suspected: Cybercrime is an incredibly lucrative business for the bad guys, and both enterprises and governments aren't doing enough to protect themselves. Our first 'Into the Web of Profit' report, published in 2018[1], exposed how the cybercrime economy generates a whopping **$1.5 trillion in revenue each year** – a number that will very likely continue to increase – with some of the funds being reinvested into traditional crime, including human trafficking and terrorism.

Yet the most interesting, and perhaps, unexpected notion to come from the report, is the identification of a new form of cyber-enabled crime – platform criminality – whereby cybercriminals are mirroring the disruptive platform-based business models utilized by the likes of Uber and Amazon, and where data is the number one commodity. For all that's good about the clear web, there's a mirror image that's nefarious, unregulated, and dangerous.

In this report, Dr. McGuire takes us through the looking glass of the dark net to examine how platform criminality is inspiring a new wave of services that target the enterprise. Dr. McGuire's findings shed light on the dark web; it's a veritable candy store for cybercriminals looking to steal IP and data, trade in secrets, disrupt operations, or spy on the enterprise.

Hackers-for-hire mean business: They infiltrate organizations, build sophisticated networks to destabilize the enterprise at-scale, and create tailored malware. These findings reveal how determined today's cybercriminals are when it comes to achieving their goals, shedding light on the methods and techniques they use to defraud individuals and enterprises.

The increasingly tailormade and targeted nature of the dark net services should act as a wake-up call to the significant risks for business, covering everything from competitiveness and revenue protection, to reputation and business continuity. The most overt, risky, and worrying trends should light a fire under the enterprise:

1. **It's a seller's market for custom malware:** Requests for bespoke malware outstrip 'off the shelf' versions 2:1, with an increased demand for zero-day, polymorphic malware, and malware tailored to specific industries. For organizations, this means the specter of customized threats never seen by detection-based security tools could hit enterprise IT assets at any time, slicing through defenses like a hot knife through butter.
2. **Targeted access to business:** Many vendors offer access to individual businesses, with more than 60% offering a gateway into 10 or more corporate networks – with financial services and healthcare organizations being the most popular. Others offer espionage services that seek to obtain corporate data or other valuable IP stored digitally on enterprise assets.
3. **Spoofing linked to phishing:** Whether it's cheap spoof pages for eBay, Amazon, and Minecraft, or $40 full-service phishing kits, dark net shoppers can buy everything they need to target the enterprise with mass-phishing campaigns. More concerning is the ready availability of invoices and other official documentation that is often used to hoodwink unsuspecting employees into triggering malicious executables.

The volume of cybercrime is so massive, it has been described as the largest and fastest transfer of wealth in history – despite more than a trillion dollars that commercial and government

[1] Into the Web of Profit, April 2018

organizations are expected to spend on cybersecurity products and services cumulatively from 2017-2021[2]. We can do better. Cybercriminals always seem to be a step ahead of enterprise security efforts, and a growing proliferation of dark net platforms is making it easier for them. Only with a thorough understanding of the risks posed by threats on the dark net can we hope to combat their tactics and disrupt their networks. But to do that, the enterprise needs to completely rethink security, deploying layered defenses that go beyond detection – only then can legitimate businesses tip the balance in their favor. If we don't, then we'll never stem the tide of threats, or the lucrative trade in secrets and business-critical data on the dark net.

[2] Cybersecurity Ventures 2017, https://cybersecurityventures.com/cybersecurity-market-report/

EXECUTIVE SUMMARY

Dr. Michael McGuire,
Senior Lecturer in Criminology,
University of Surrey

The dark net or dark web (henceforth 'dark net' in this report) has acquired a sinister reputation as one of the most active domains for cybercriminality[3]. Yet, while its role in furthering digital crime has been widely discussed, less scrutiny has been applied to its impact upon the enterprise.

In this report, we examine the developing relationship between the enterprise and the dark net, both positive and negative, specifically looking at:

(i) The criminal risks and other challenges posed by the dark net to the enterprise

(ii) The 'grey net' and how enterprises are occasionally operating at the margins of the law in utilising its resources

(iii) The emerging opportunities the dark net offers to organisations – and the kinds of precautions required to take advantage of these opportunities

For this report, we embedded researchers within gated and private platforms and communities within the dark net. This gave us unique insights into how cybercriminals target enterprises and helped expose conversations with 'vendors' of cybercrime services. This study also features examples of advertisements and services offered on the dark net, interviews with more than 30 cybercriminals, and insights from a global panel of experts – including law enforcement, security professionals, and other third-party specialists.

The term 'dark net' is used interchangeably with the term 'dark web'. It refers to online content that is not accessible by standard browsers, like Google Chrome (sometimes called the 'clear net') but may be accessed through specialised dark net search engines.

From the availability of traditional crimeware services that offer disruption and access to enterprise networks (such as malware, remote access Trojans (RATs), phishing, and so on), through to more subversive forms of influence (such as corporate espionage, insider trading, and whistle-blower blacklisting) – it is evident the dark net is a growing threat to the enterprise. The market for specialised tools and information designed for targeted attacks on enterprises is also widening; we noticed a growing demand for tailored attacks against individual targets within corporations, with hackers offering information on everything from financial performance to security systems, and even internal product manuals.

Another key finding is the shift towards an 'invisible net' – invitation-only platforms and private forums and messaging networks where interactions between members are shielded from law enforcement. In fact, 70% of dark net service providers invited our undercover researchers to talk over private, encrypted channels in the 'invisible net'. This is making it harder than ever for law enforcement to track dark net transactions and for enterprises to defend themselves. Most enterprises are simply not prepared to respond to rapidly changing attack vectors, and current forms of security and policing are often insufficient to deal with increasing threats. Ultimately, the dark net as a source of threat to the enterprise, as well as an enabler of cybercrime, requires greater examination if we are to establish more robust systems to tackle the risks it poses.

[3] The term 'dark net' is used interchangeably with the term 'dark web'. It refers to online content that is not accessible by standard browsers, like Google Chrome (sometimes called the 'clear net') but may be accessed through specialised dark net search engines. The dark net is usually distinguished from the deep net/deep web, which refers to online content not directly connected to the rest of the internet, but which can only be accessed by using special passwords or other credentials – for example, government databases, library catalogues, or commercial intranets

THE STORY IN STATISTICS

- Our findings show that compared to 2016, there has been a 20% rise in the number of dark net listings that have a potential to cause harm to the enterprise. These include increases in targeted malware for sale, enterprise-specific DDoS services, corporate data for sale, and brand-spoofing phishing tools.
- 70% of vendors that our researchers engaged with invited us to talk over private channels in the 'invisible net'.
- 60% of listings analysed (excluding drugs) represented opportunities for direct harm to enterprises – potentially causing immediate and tangible damage, such as network compromises, suspension of online services, or financial loss.
- 15% of listings represented opportunities for indirect harm to enterprises – including longer-term, more abstract damage, such as brand dilution or reputational harm. A further 25% of listings involved items that could cause both direct and indirect harm – such as counterfeit goods.
- Two-thirds of the listings analysed, which included a range of network, financial and data compromise tools and services, such as remote access, were characterised as posing a high level of threat while the likes of refund fraud were classed as medium.

NETWORK COMPROMISES:

- Malware, DDoS and RATs were the most common types of network compromise services available on the dark net – accounting for 25%, 20%, and 17% respectively of all listings relating to network compromises.
- At least 60% of vendors questioned in relation to network access offered access to more than 10 enterprise networks; 30% offered between five and 10, and 10% were offering up to five.
- Remote access credentials were found to be retailing at $2-$30 each.
- The cost to purchase targeted attacks on enterprises averaged around $4,500, compared to $2,000 for targeted attacks on individuals.
- The most expensive malware found retailed at $1,500; it targets ATMs.
- Around 40% of attempts by our researchers to request dark net hacking services targeting companies in the FTSE 100 or Fortune 500 received positive responses; prices ranged from $150-$10,000 depending on the company involved.

FINANCIAL COMPROMISES:

- Credentials, phishing and fake receipts to obtain refunds were the most common types of services offered in relation to financial compromises – equating to 38%, 27%, and 14% respectively of listings.
- Pages suited for phishing were for sale for just $0.99, with full-service phishing kits for sale off the shelf, starting at $40; fake Amazon receipts and invoices that could be used to obtain refunds were found for sale for as little as $52.

DATA COMPROMISES:

- Consumer account details, consumer bank logins, and business email addresses were the most common types of data compromises that researchers found – representing 28%, 21%, and 15% respectively of listings analysed in this subset.
- Espionage services (e.g. access to the CEO) were offered to researchers for fees ranging from $1,000-$15,000; researchers also made contact with multiple individuals offering insider trading tips.

INTRODUCTION

CATCHING SMOKE - THE CHALLENGES OF NAVIGATING THE INCREASINGLY INVISIBLE NET

Finding one's way around the dark net often feels like entering a hall of mirrors in a dense fog. Not only is it inaccessible to familiar search engines, like Google, but sites come and go very quickly, often due to disruption from law enforcement. However, these takedowns do not end dark net trading, they merely disrupt it temporarily. For example, new or cloned versions of seized sites opened almost immediately after the takedown of Silk Road and AlphaBay; listings across other dark net platforms increased up to 28% the following week, according to reports[4], whilst many other lower profile sites remained active.

Not only is the dark net pervasive, it is also increasingly secretive – more than 70% of the vendors we interacted with either invited us to talk over private channels or told us that they were now operating exclusively through private or encrypted messaging systems. The development of this 'invisible net' of online interaction is supporting the emergence of new, still more covert forms of cybercrime – which are likely to parallel, and eventually maybe even outstrip crime on both the clear and dark nets. This has as many worrying implications for the enterprise, as it does for researchers and law enforcement, as dark net activities are driven even further underground. The dark net represents a significant risk to the enterprise that many organisations are simply unprepared for, arming adversaries with all the tools and skills they need to steal data and disrupt businesses at will.

1. THE DARK NET ECONOMY - PLATFORMS, COMMODITIES, AND PROFITS

As with the clear net, platforms are central to the flow of trade on the dark net. While the reputation of the dark net as a haven for drug sales is not without justification, the findings of this research suggest that enterprises are also vulnerable to a whole range of threats on the dark net. In fact, by utilising available archives of dark net platforms[5], we estimate there has been a rise of around **20%** in listings containing potential threats to the enterprise when compared to similar listings from 2016. These include increases in targeted malware, enterprise-specific DDoS services, corporate data for sale, and brand-spoofing phishing tools.

Of the 70,000+ listings examined[6] in this research, 47% were related to drug or drug-related sales, while just under half (43%) were related to digital products like compromised bank accounts, malware, DDoS tools, or stolen card credentials. Six percent represented 'services' like hacking tutorials, and around 4% were other items. Excluding content related to drug sales, we found that:

- **60%** of the digital products and services traded on the dark net represented direct opportunities to harm the enterprise.
- **15%** of content could be associated with more indirect forms of harm to the enterprise (e.g. reputational damage).
- The remaining content (around **25%** of the total) involved items such as counterfeit goods. Whilst illegal and potentially damaging in the long term in terms of brand dilution, this content was of less immediate concern to the enterprise.

It is evident that the threat posed to enterprise from the dark net is significant and rising.

---

[4] Kelion (2017)
[5] See Branwen (2019) for one source
[6] See the methodology for more detail about the listings and platforms examined

1.2 - THE MULTI-DIMENSIONAL RISK POSED BY THE DARK NET TO THE ENTERPRISE - A 3D THREAT ASSESSMENT

To gain a more substantive sense of what these criminal threats might amount to for the enterprise and to better understand their multidimensional nature, we developed a 3D dark net threat assessment tool[7] to measure the potential damage to the enterprise from 12 categories of dark net tools or services that expose enterprises to potential network, financial, and data compromise. These 12 categories include:

- Infection/attacks (including malware, DDoS, and botnets)
- Access (including RATs, keyloggers, and exploits)
- Espionage (including services, customisation, and targeting)
- Support services (such as tutorials)
- Credentials
- Phishing
- Refunds
- Customer data
- Operational data
- Financial data
- IP/trade secrets
- Other emerging threats

Damage caused by each of these 12 attack vectors was analysed by an expert panel that looked at examples from each of these groups of dark net tools and assigned scores to them on the scale of 0 to 30 on three key variables, to determine the level of overall impact they could have on the enterprise. These variables are as follows:

1. **Devaluing the enterprise:** For example, the undermining of trust in their brand, loss of status and reputation, or handing advantage to a competitor.
2. **Disrupting the enterprise:** For example, DDoS attacks or other malware that creates disruption to business operations.
3. **Defrauding the enterprise:** For example, data or IP theft or espionage, which can impact a company's ability to compete or cause direct financial loss.

The outcomes (which are detailed in the upcoming sections) are concerning. In eight of the 12 threat categories that were analysed, the enterprise is confronted by **high** levels of threat. **Medium** levels of threat are posed by the remaining four categories, with no categories indicating low or negligible levels of threat.

When a category emerged as a high-level threat for the enterprise, this meant the potential for damage through either disruption, devaluing, or defrauding was rated as acute, posing significant risks to the ongoing viability and long-term sustainability of the enterprise as a whole. By contrast, medium-level threats, though harmful, were less likely to result in risks to the capacity of the enterprise to continue working.

[7] See the methodology for more detailed information on how this tool was developed

Threats were evaluated on a scale of one to 10 for each category, producing a possible total score of **30**. Scores were then correlated with threat levels as follows:

20 – 30: High threat level

10 – 19: Medium threat level

0 – 9: Low threat level

1.3 - TOOLS AND SERVICES BEING SOLD TO ENABLE COMPROMISES OF ENTERPRISE NETWORKS

We looked at four broad categories of commodities being traded across dark net platforms that may compromise enterprise networks. These are indicated in the table below, along with typical items within each category, the average percentage of listings for items in each category[8], an average price for each item, and the 3D enterprise threat assessment rating for the category as a whole[9].

CATEGORY	ITEM	AVERAGE %	AVERAGE PRICE $	3D THREAT SCORE	3D THREAT LEVEL
Network Compromises					
Infection / attack tools	Malware/Malware services	25	3-40	**22**	**High**
	DDoS/Botnet services	20	20		
Access	RATs	17	2-30	**27**	**High**
	Exploits	7	100+		
	Keyloggers	6	5		
Targeting and espionage	Targeting services	9	15-50+	**26**	**High**
Support services	Tutorials	12	6	**18**	**Medium**
Other	-	4	-		**Unrated**

Table 1: Network compromise tools and services on the dark net

1.3.1 INFECTION/ATTACK TOOLS

We studied a range of tools and services that can enable infections or attacks upon corporate networks. By analysing forum discussions and correlating this with feedback from vendors and hacking service providers, we were able to identify the types of tools most frequently used to target enterprises. Not surprisingly, malware and DDoS/botnet tools represent the most frequent types of threat from the dark net in relation to network compromises; constituting an average of around 45% of listings examined (25% for malware and 20% for DDoS).

The research uncovered a worrying trend — an increase in the destructive power in some malware strains found on the dark net. For example, the Nuke malware[10] can open remote desktop sessions and destroy any rival malware found on its target system. This allows a criminal to take over a machine, negate other malware, and gain almost total control over it. More worryingly for

[8] Calculated by treating each domain as 100% and excluding other items listed on dark net platforms. Drugs were not included within any category because the volume sold is significant and can obscure some of the more subtle variations within each category

[9] The 3D threat assessment scores can be found in the Methodology section of this report

[10] Darkweb news (2017)

the enterprise is that it can bypass many kinds of Windows firewall protections. We found several examples of this strain for sale, especially on Russian-language forums, where it was often being promoted as an ideal attack tool against enterprise networks.

The use of new and harder-to-detect channels for mounting attacks and managing malware was also identified. For example, the shift towards hiding DDoS command and control on the dark net or the use of invisible net mechanisms to manage software like the Katyusha Scanner, which can scan websites for potential SQL injection vulnerabilities using just a smartphone and the Telegram messaging app. This also raises the risk of 'on site' attacks by business insiders using only their smartphone.

Our research also identified which verticals were most frequently targeted by the infection or attack tools traded on the dark net. The breakdown can be seen in Table 2 below. Banking and e-commerce businesses emerged as the most targeted verticals, followed by the healthcare and educational sectors.

MOST FREQUENTLY TARGETED INDUSTRIES

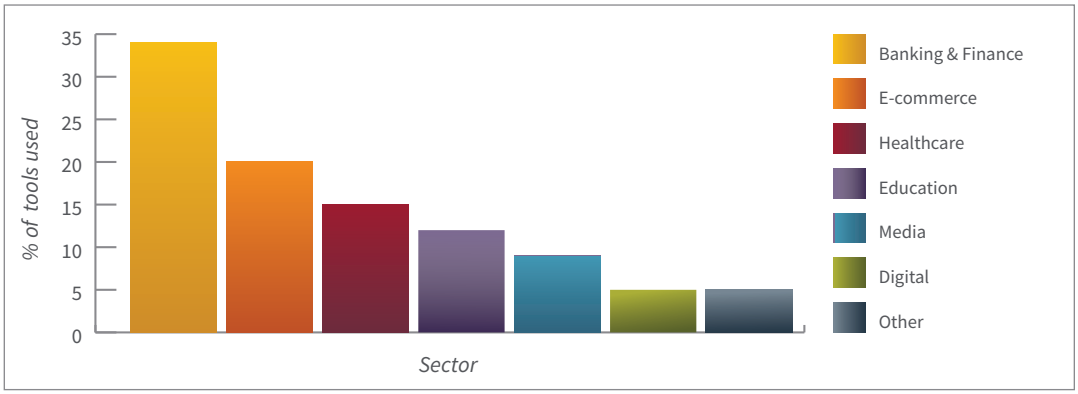

Table 2: Enterprise sectors most frequently targeted by dark net infection/attack tools

1.3.2 ACCESS

Within every dark net market that we examined, vendors offered ways to access specific enterprise networks. The methods varied considerably; some involved stolen IT admin credentials, others offered malware like RATs. Our researchers were also offered 'backdoors' into networks – though details of these were refused until a substantial upfront fee was provided. At least **60%** of the vendors questioned were offering access to more than 10 business networks, **30%** were offering access to between five and 10 networks, and **10%** were offering access to up to five networks.

The refining of some malware strains to make them more suitable for attacks upon the enterprise was also apparent. For example, upgrades to RATs like the AZORult malware, originally designed for stealing credit card information, now provide purchasers with a more user-friendly admin control panel, together with a lower anti-virus detection rate, ideal for evading many detection systems used by enterprises.

[11] Infosec (2018)

However, an increasingly common way of acquiring access doesn't involve malware. Instead, access can be obtained by way of remote access credentials, such as the Remote Desktop Protocol (RDP) — a Microsoft protocol, typically used to manage remote computers over the network. But bad actors have developed ways to exploit RDP sessions to steal login credentials and demand ransom for valuable information, often evading detection by the usual enterprise protections.

Our research found numerous sources across dark net platforms where credentials could be purchased for $2-$30 each. There are even RDPs permitting access to airport security found on the dark net[12]. This finding has been corroborated by other researchers, with access to systems in China and South America proving especially popular. The Ultimate Anonymity Services (UAS) platform alone was found to be selling more than 7,000 credentials from China and 6,000+ from Brazil. RDPs in the US were also available, especially from California, Ohio, Oregon, and Virginia[13].

When looking at access, the research showed a preference for RATs over keyloggers and exploits. On average, we found or were offered RATs around five times as often as we found or were offered keyloggers and exploits. RATs allow criminals to exert control over a network from a distance, enabling hackers to do things like activate webcams, take screenshots, monitor user behaviour, or access sensitive information, such as credit card numbers.

It is evident from the listings that this type of attack is back in vogue. For example, the Ramnit banking Trojan, which can steal banking credentials, though first detected in 2010, became the most prevalent threat to banks in 2018. A wave of attacks against West African banks utilising RATs were detected between 2017-2019[14].

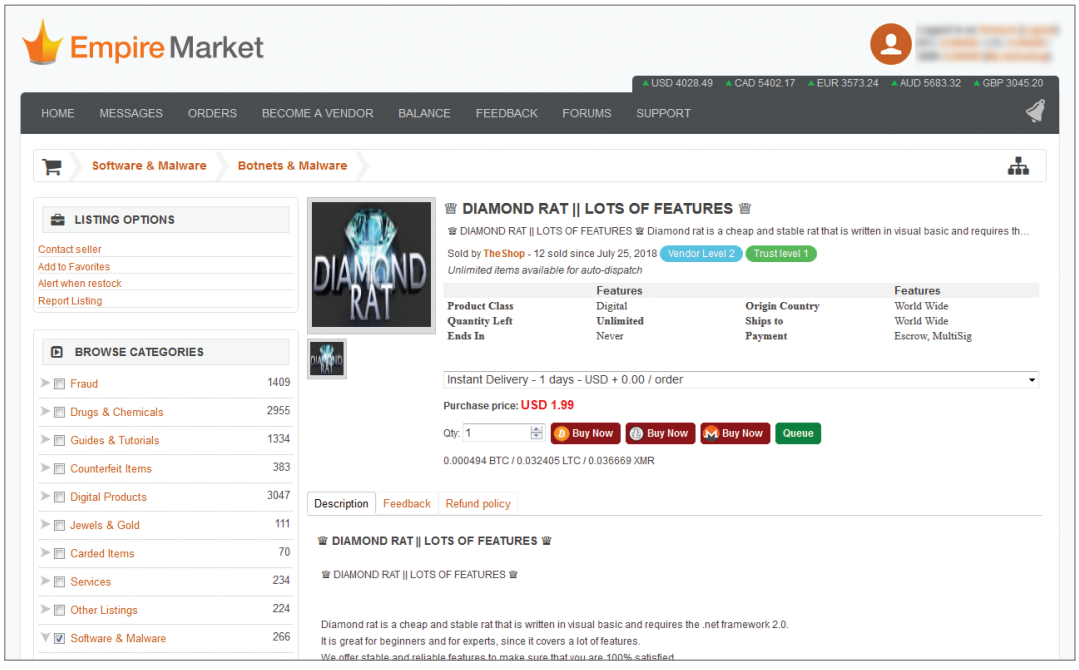

Fig.1 Popular strains of RATs are retailing for around $10, but cheaper versions, like the 'Diamond Rat', retail for only $2

Popular strains of RATs, like DNS Messenger, are retailing for around $10, but we found cheaper versions, like this 'Diamond Rat' that could be used to operate desktops remotely, retailing at $2. In general, the price tends to increase as the tool becomes more system-specific[15].

Versions that operate across Macs – such as MacSpy, which can monitor much of a Mac users' data – appear to be virtually undetectable and represent a particular risk to often Mac-based creative industries[16]. Elsewhere, new

[12] Zorz (2018)
[13] Trend Micro (2017)
[14] Ilascu (2019)
[15] Migliano (2018)
[16] Paganini (2017)

RATs utilising the Android system have been found to exploit the Telegram messaging service, permitting criminals to send SMS messages, record calls, and even install apps[17].

Vendors offer access to a diverse range of business networks. Access to networks in the healthcare, banking, and retail/e-commerce sectors appeared to be especially prevalent, as indicated in Table 3 below.

VERTICAL	% OF VENDORS OFFERING ACCESS
Healthcare	24
Banking	18
E-commerce/retail	16
Education	12
Finance	11
Other	19

Table 3: Vertical markets that dark net vendors are offering access to

1.3.3 TARGETING AND ESPIONAGE

When it comes to targeted attacks, it's a seller's market for malware on the dark net. We found far more requests for custom malware, compared to offers for off-the-shelf versions, which supports suggestions elsewhere that requests for malware creation may exceed what is actually on offer by around 2:1.

Almost every vendor offered us tailored versions of tools, which they said would 'work better' depending upon the network we wanted to access or damage; the more targeted the attack, the higher the price. And prices rose still further where potential attacks involved high-value enterprise targets, such as banks.

Targeted attacks on enterprises averaged around $4,500, higher than costs of attacking individuals (approximately $2,000). For example, one potential buyer on the Empire Market dark net was requesting services targeted against PayPal or individuals who use PayPal, and was offering up to $2,500 to anyone who could provide access to user accounts and block them from sending and receiving money.

One of the most expensive pieces of malware found was designed to target bank ATMs (via ATM logic attacks) and retailed for approximately $1,500[18]. This was a little surprising given that ATMs are hardly the most modern way to access money and there are cash limits upon them. When questioned about this, one vendor simply said "the old ways are sometimes the most reliable ways. And the risks of detection are far lower".

Around **40%** of attempts by our researchers to request dark net hacking services targeting companies on the FTSE 100 list or US companies on the Fortune 500 list received positive responses. In almost every case where a request to target a specific company was made, vendors also responded positively, with many offering a variety of service plans for conducting the hack. Negotiated prices were between $150-$10,000, depending upon the company involved.

[17] Vigliarolo (2018)
[18] See Infosec (2018) for corroborated findings

The volume of targeting services suggests that there is high demand for spying on company activities. FBI data highlighted a 53% growth of investigations related to possible economic espionage over a 12-month period in 2015-2016 targeting US businesses[19].

It was difficult to obtain data on espionage within the relatively open context of forums, so we took steps to learn more:

(i) Asked vendors providing hacking services whether they would be prepared to engage in directed or targeted espionage. As our earlier findings suggested, around 60% of vendors we questioned claimed to be offering access to specific networks.

(ii) Put out a communication on the Telegram messaging service to explicitly request espionage activities for a specified fee. Within 48 hours we had received 30 responses expressing an interest but, for legal reasons, those offers were not taken any further.

In general, we found that where espionage does occur, it takes two forms:

(i) Simple spying: Where individuals seek to acquire confidential information for their own benefit. The aim here is usually financial gain.

(ii) Surrogate spying: Where the attempt at espionage is conducted on behalf of another – usually a client. In sections 3 and 4 we consider the extent to which enterprises themselves may be engaging in such activities, but other clients – such as nation states – cannot be discounted.

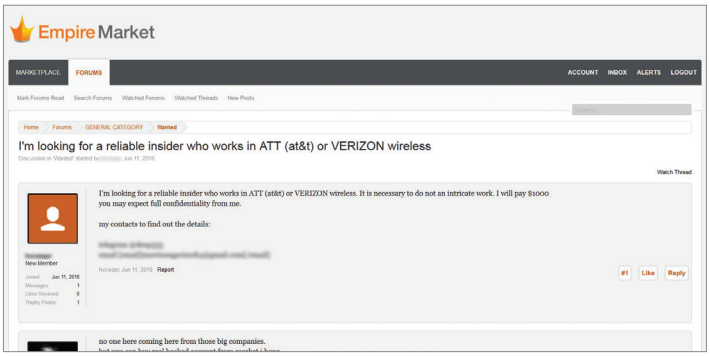

Fig.2 A member of the Empire Market site is looking for insiders to gather information on AT&T and Verizon

During our research, we found instances of attempted spying instigated by individuals who were looking for access, often by way of recruiting insiders. As illustrated in Figure 2, an individual was looking for company insiders at either AT&T or Verizon; when contacted, they were largely interested in details of company contracts and payroll arrangements.

Finding definitive evidence of enterprises engaging in spying against each other is far harder, and establishing the extent to which the dark net might have facilitated this is even more uncertain. Not surprisingly, even on the dark net, enterprises are unwilling to provide any concrete indications of being eager to engage in illegal activity of this kind.

As a result, though the research found evidence of company secrets for sale across the dark net, there was no direct evidence to be found that it was the enterprise itself that was responsible for this. As the next report in this series will detail, there is also compelling, though hard to verify, evidence of nation states as perpetrators of industrial espionage. For example, theft of US corporate secrets by China has been estimated to cost up to $600bn per year[20]. With such high volume of threats readily available, organisations need to be vigilant to ensure they don't fall victim to espionage.

[19] Kahn (2018)

[20] US IP Commission (2017) http://ipcommission.org/

1.3.4 SUPPORT SERVICES

At a lower level of threat, yet still a concern, is the wide availability of tutorials that teach viewers how to launch attacks. While these vendors are not launching attacks themselves, the ready access to such information can enable a new generation of cybercriminals, making it easier than ever to upskill and engage in cybercrime.

For example, posing as a 'noob' (an inexperienced hacker), we asked various service providers for help in setting us up with fully tailored hacking systems. The vendor 'sixandeight' offered to provide us with a complete system for engaging in carding.

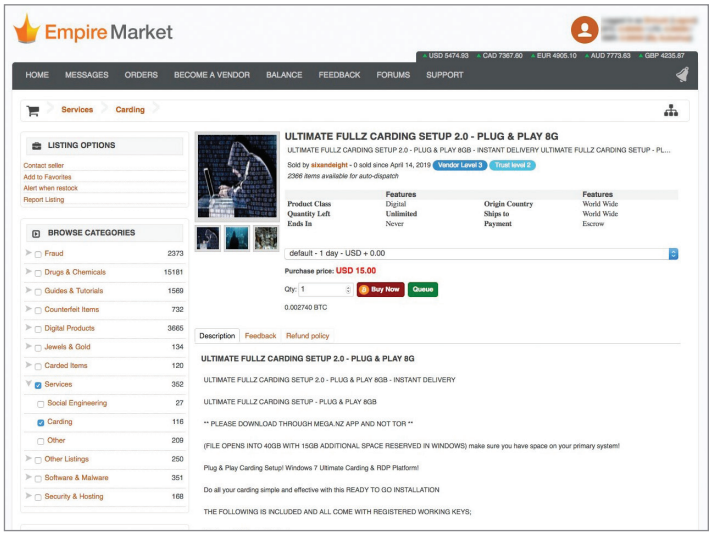

Fig.3 A vendor on the Empire Market site offered to provide us with a complete system for engaging in carding

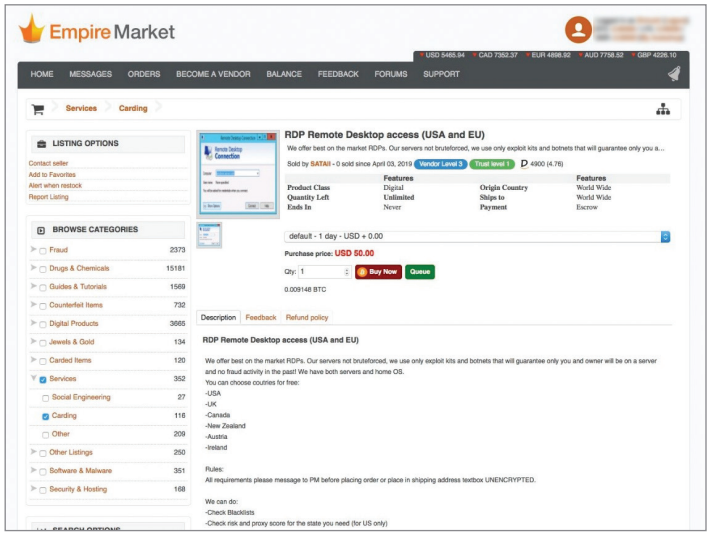

Fig.4 A vendor is offering a range of remote desktop protocols, complete with extensive support and the use of clean servers

Similarly, the vendor "SATAII" was offering a range of remote desktop protocols, which came with extensive support and the use of clean servers in the country of our choice with no record of fraud activity in the past.

It is also evident that there is an increasing focus upon personalisation and customer service to enable attacks. In particular, we noted a significant number of 'end-to-end' hacker services, which have begun to supersede distribution of banking-style Trojans, which are more limited in their scope.

A similar trend towards increased personalisation was seen in the emergence of specialised traffic distribution systems (TDS)[21], which allow clients to submit their own custom-built malware and get it distributed. Several vendors assured us that these systems were especially good for customised malware attacks on any business we wanted to name.

1.4 - TOOLS AND SERVICES BEING SOLD TO ENABLE FINANCIALLY MOTIVATED COMPROMISES

The sale of tools or services that can be used to extract financial value or wealth is fundamental to the cybercrime economy, which derives around 50% of its revenue from activities like fraud[22]. As a key wealth generator, the enterprise has become an obvious target, with tools for sale that either provide direct access to networks for a cybercriminal or enable others to design and

[21] See Proofpoint (2018) for some examples of how BlackTDS has been used

[22] See Web of Profit (I) for a full breakdown of cybercrime revenues

organise their own bespoke attacks. These are indicated in the table below, along with typical items within each category, the average percentage of listings within this domain[23], an average price for each item, and the 3D enterprise threat assessment rating for each category[24]. The table also includes data for financial attack tools and services discussed below in Section 3.

CATEGORY	ITEM	AVERAGE %	AVERAGE PRICE $	3D THREAT SCORE	3D THREAT LEVEL
Financial attacks					
Credentials	Credit card details	38	2+	**28**	**High**
Phishing tools	Phishing tools & services	27	5+	**28**	**High**
Refunds and other scams	Fake receipts	14	6+	**19**	**Medium**
Other	-	21	-		**Unrated**

Table 4: Financial attack tools on the dark net

1.4.1 CARD CREDENTIALS

Digital credit and debit card credentials, such as passwords, CVV numbers, and expiration dates, are the most familiar and common type of financially-focused commodity circulating across dark net markets, at around **38%** of all listings. These are cybercrime staples, but the volume of sales appears to have grown as the dark net business model moves towards larger and larger batches of data. Other studies suggest that databases of more than 1 billion credit card records have been found for sale on the dark net[25], and it has been estimated that around 40% of stolen credit card data ends up on dark net platforms[26].

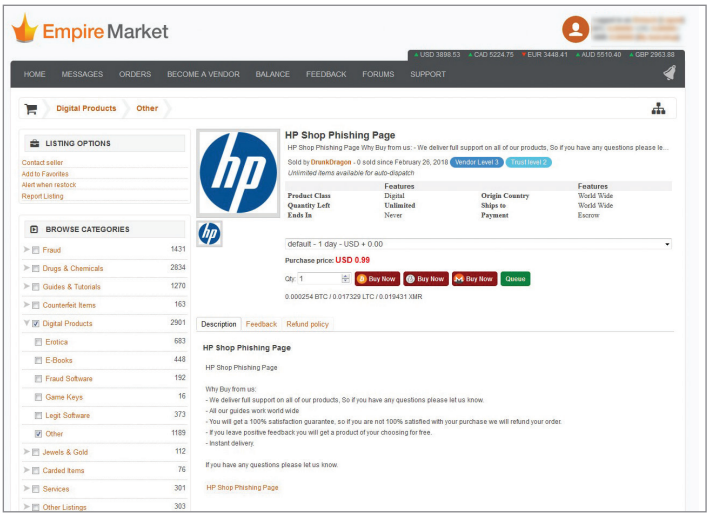

Fig.5 A vendor is offering phishing pages for HP for USD 0.99, backed by an offer of full support and money back guarantee

1.4.2 PHISHING TOOLS

The presence of phishing tools for sale on the dark net is well documented. We found that **27%** of listings across dark net markets (in the financial attacks category) were overtly related to phishing tools, and a large proportion of these could easily be used against the enterprise.

Some involved indirect exploitation, achieving their goal by luring victims into surrendering private information using expertly designed spoof pages, masquerading as popular brands. For example, the vendor DrunkDragon was providing HP or Amazon pages suitable for phishing for only $0.99. (Figure 5 and 6)

[23] Calculated by treating each domain as 100% and excluding other items listed on dark net platforms. Drugs were not included within any category because the volume sold is significant and would obscure some of the more subtle variations within each category

[24] The 3D threat assessment scores can be found in the Methodology section of this report

[25] Casal (2017)

[26] Equifax (2018)

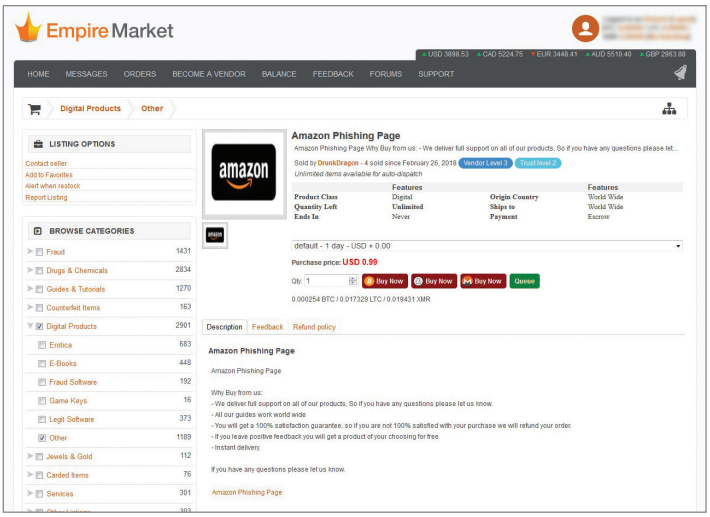

Fig.6 A vendor is offering phishing pages for Amazon for USD 0.99. The product description suggests that four such pages have been sold already

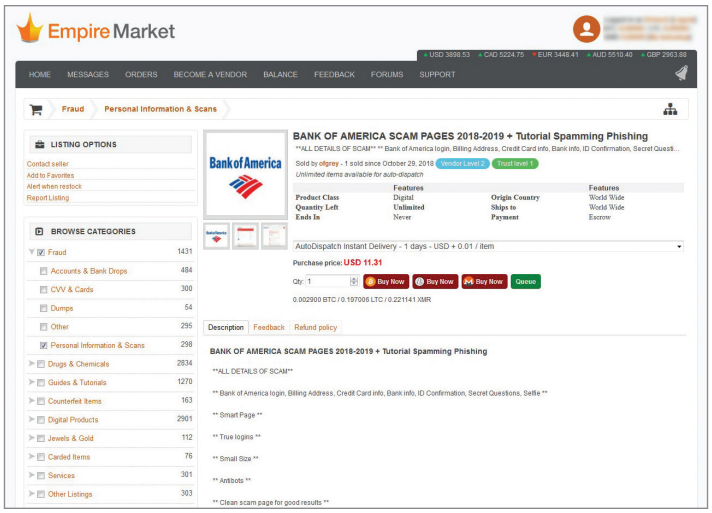

Fig.7 A Bank of America spoof website pages are being offered, complete with tutorial support, for $11

Elsewhere, the vendor Ofgrey was offering Bank of America spoof website pages together with tutorial support for $11. (Figure 7)

Our researchers found numerous other examples, with pages pretending to originate from companies like Apple and Netflix, and popular retailers like Tesco and Walmart. Spoof pages from gaming sites like Minecraft and League of Legends were also among the popular ways of persuading potential victims to click on phishing links. Such pages can be sold for as little as a couple of dollars, though pages for more in-demand or higher status pages, like Apple, usually retailed for more.

Other tools were more developed, with an emerging trend involving full-service phishing kits, which are sold off the shelf for around $40 and up. These advanced phishing kits provide customers with tools they can use to build their own spoof sites for harvesting data.

Other examples include the [A]pache phishing kit, targeted at South American users, which offers extensive capabilities to create domain names similar to the spoofed site (e.g. Walmart-shopping.com). The kit also contains many other small details designed to entice victims into believing it is real – for example, an automated postcode look-up function[27].

Phishing attacks targeted at enterprises can be very costly. For example, a phishing email campaign in 2017 conducted by the Carbanak cybercrime group was aimed at US restaurant chains like Chipotle, Arby's, and Chili's. More than 15 million credit card details were stolen, resulting in millions of dollars in damages. The attack was carried out by persuading restaurant staff to click on links in the emails that appeared to contain catering orders or other matters relevant to the business[28].

1.4.3 REFUNDS AND OTHER SCAMS

We found evidence of a thriving dark net market that entices organisations to hand over money through fraudulent refund requests. Visa has suggested that more than 80% of all chargebacks are fraud-related, and enterprises stand to lose around $25 billion through this method by 2020[29]. Access to stolen card details can be an important driver of chargebacks or 'friendly' fraud, where

[27] Wiat (2018)
[28] Ng (2018)
[29] Chargebacks (2019)

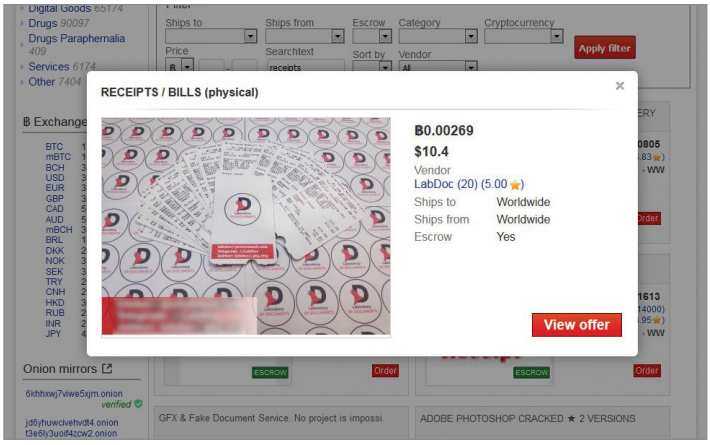

Fig.8 A vendor is offering to provide physical copies of any type of receipt

a criminal makes an online purchase, often with credit cards they have acquired via dark net platforms, and then disputes the charge to their credit card. The bank is then compelled to issue a refund and the customer keeps their illicitly gained purchase.

The provision of fake receipts and other documentation for obtaining refunds was another popular approach. For example, we contacted a vendor called LabDoc who boasted that they could produce physical copies of any kind of business receipt or bill. (Figure 8)

Similarly, a Russian vendor called Den was found to be providing invoices for Amazon and Apple so that refunds could be obtained. (Figure 9 and 10)

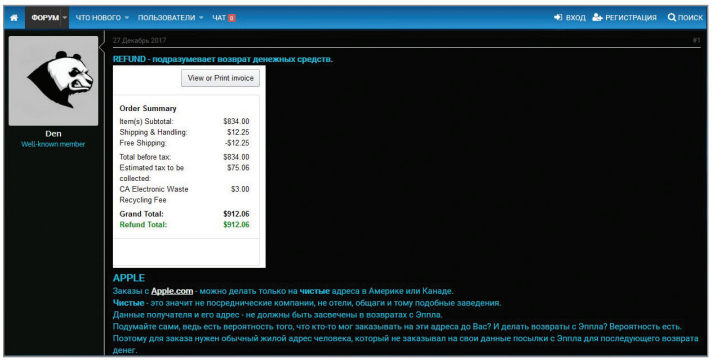

Fig.9 A Russian vendor is providing invoices for Amazon and Apple so that refunds could be obtained

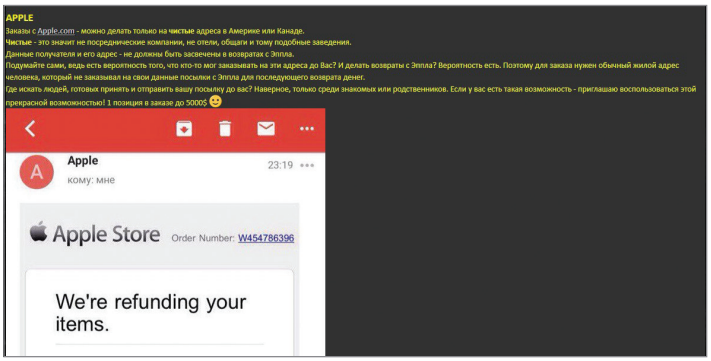

Fig.10 A Russian vendor is advising his potential customers to use "clean" home addresses of real people to avoid being flagged by Apple as a frequent return customer

1.5 - TOOLS AND SERVICES BEING SOLD TO COMPROMISE DATA

In many ways, the dark net trade in data has become as much of a threat to the enterprise as the trade in crimeware. Our research suggests that data is the second most prevalent item traded across dark net platforms – after drugs – and the sheer range of data types now available on the dark net is staggering.

Our research, together with other estimates, suggests that 25-33% of dark net activity relates to the buying and selling of corporate data[30]. The damage can involve a strong combination of devaluation, disruption, and defrauding, including: depreciation in the value of the data, loss of customer faith, loss of staff morale, a rise in negative perception of the company, and additional expenditure on security to plug gaps where data has been breached.

Attributing culpability for the leaking of data is, however, a highly uncertain affair. There is certainly evidence that individual perpetrators are willing to pass on sensitive information – company insiders have been implicated in at least half of data breaches[31], with the majority of breaches resulting in data theft traceable to lower-level employees, rather than senior management or IT.

[30] Filecloud (2018)
[31] Allen (2018)
[32] Preston (2019)

However, significant risk is also posed by higher-ranking former employees who leave for a competitor. Sometimes their acquisition of sensitive information can be very easy, with up to 13% of employees who switch jobs thought to be able access their old employers' networks using their original credentials[32].

Other risks come from employees who can bring their own devices into the workplace (BYOD) and who simply copy data and files before they leave. As a result, many businesses now require employees who handle sensitive information to complete a 'non-compete' clause, which requires them not to gain employment with business competitors or to start their own business using the enterprise's information.

We found four broad categories of company data openly traded across dark net platforms. These are indicated in the table below, along with typical items within each category, the average percentage of listings within the overall volume of data listed, an average price for each item, and the 3D enterprise threat assessment rating for each category[33]. This excludes other items listed within other categories on dark net platforms.

CATEGORY	ITEM	AVERAGE %	AVERAGE PRICE $	3D THREAT SCORE	3D THREAT LEVEL
Data theft					
Customer data	Account details	28	10	**25**	**High**
	Bank/other logins	21	5		
	Correspondence	4	20		
Operational data	Business emails	15	10-50	**17**	**Medium**
	Internal communications	5	35		
Financial data	Invoices	14	5-10	**23**	**High**
	Annual accounts	6	60+		
Trade secrets and IP	All kinds	Unclear	Unclear	**16**	**Medium**
Other		7			**Unrated**

Table 5: Company data being traded on the dark net

1.5.1 CUSTOMER DATA

When customer details are found on the dark net, it can create major headaches for enterprises, resulting in damaged trust, reputational damage, disruptions to trading, revenue loss, time and money for remediation, even, potentially, share price drops and loss of investor confidence.

For cybercriminals, financial data is clearly a high priority, and the reported 135% rise in the trading of customer data (such as account logins and credit card information) from banks between 2017-2018[34] is indicative of its continuing appeal.

[33] The 3D threat assessment scores can be found in the Methodology section of this report
[34] IntSights (2018)

Phishing or account takeovers are just some of the ways in which cybercriminals can use stolen data. But compromised customer data has more general uses too. For example, conversations with one dark net vendor indicated that he wanted:

> *"…customer data – any kind coz they just giving us lots of what we need by putting it altogether [sic] in nice fat databases. Find out someone is a credit card user then you got whether can they have their own place or if they rent it, you know if they're married, got kids – and how many of them. You can find out their job, earnings, even where they went to college."*

Another vendor who specialised in ransomware or online threats said he had found out:

> *"…political stuff, financial investments even where people like to travel – all very profitable for me."*

During our research we discovered a wide variety of companies whose customer data was being traded on the dark net. Some of the examples involved databases from banking or financial institutions, such as this database from the Qatar National Bank, which included customer passwords and PIN numbers.

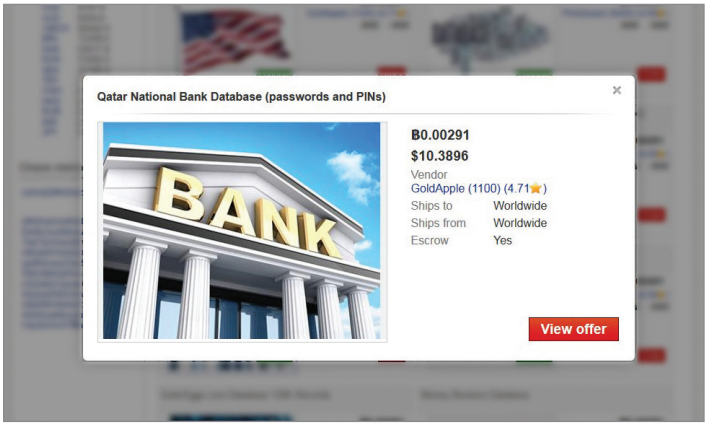

Fig.11 A database from the Qatar National Bank, complete with customer passwords and PIN numbers, for sale on the dark net

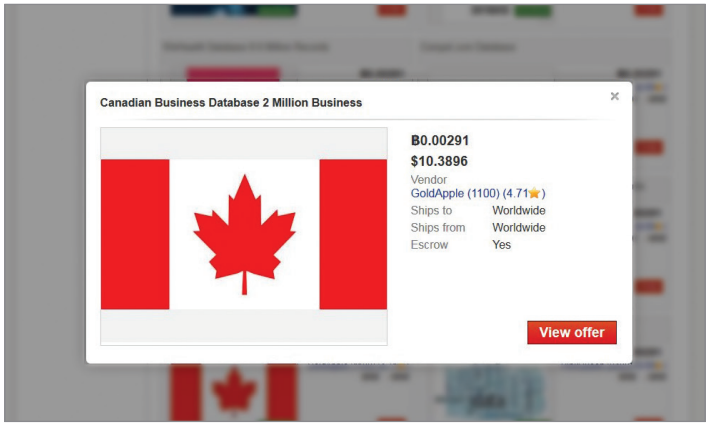

Fig.12 A vendor on the dark net offering a database of more than two million Canadian businesses for just $10

Most shockingly, we discovered databases for whole nations – such as in this example, which included data on more than two million Canadian businesses – retailing at not much more than $10.

1.5.2 OPERATIONAL DATA

Whilst the discovery of customer databases for sale on the dark net can be embarrassing for an enterprise to deal with (not to mention costly), the trade of more sensitive operational data can prove to be even more concerning. Typical commodities our researchers found available for sale included company emails, accounting and financial information (such as company invoices), and even minutes from company meetings. Around **15%** of all data traded across the dark net that we found involved corporate email chains, including content related to corporate policy or strategy, as well as payments, hiring, firing or resignation of employees, project costs, and so on. This kind of data provides lucrative options, from threats to leak information to the media, to even blackmailing of company executives.

FBI data suggests that globally, there has been a 136% rise in business email compromise scams between 2016-2018, causing more than $12bn in losses to the companies involved – usually as a result of compromised emails being used to request funds transfers[35]. They can also be used to enable more sophisticated fraud that targets specific enterprises and their corporate accounts payable departments. The research found substantial evidence of compromised corporate emails all over the dark net. Our researchers were offered a batch of Outlook emails from an online retailer, and in some of the sample emails shown to us (as enticements to purchase the whole set) we found a variety of sensitive details, including discussions of the enterprise's annual report, firing and hiring policies, team building events, and even communications relating to a covert office romance (with obvious potential for blackmail).

1.5.3 FINANCIAL DATA AND STOLEN INVOICES

Corporate financial data, like the background information that goes into annual financial reports, sells at a premium on the dark net. Our researchers were offered a selection from several leading enterprises, though these were expensive, and the vendors disappeared when we tried to follow up.

Purchasing corporate invoices is easily done on the dark net; the examples we looked at appeared to be genuine, some even came with folds and other signs of wear and tear. When we asked what these could be used for, the vendor described how to use them for phishing scams:

> *"You can also email a company one of my fake invoices which show you've bought something from whatever company you want. For an extra 0.184 XMR ($10) I can provide you with a link in the email which tells the company to click it if they did not authorise the purchase. As soon as they do, you can get all their details."*

Again, a wide variety of enterprises were represented in this trade. For example, the vendor Goldapple was offering T-Mobile invoices at $5 apiece.

The same vendor was selling Cathay Pacific invoices for around the same cost.

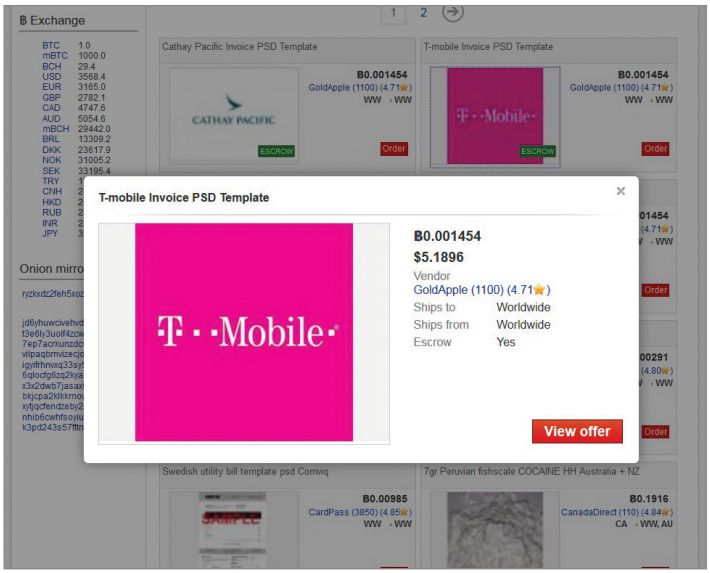

Fig.13 Counterfeit T-Mobile invoices are offered for $5 apiece

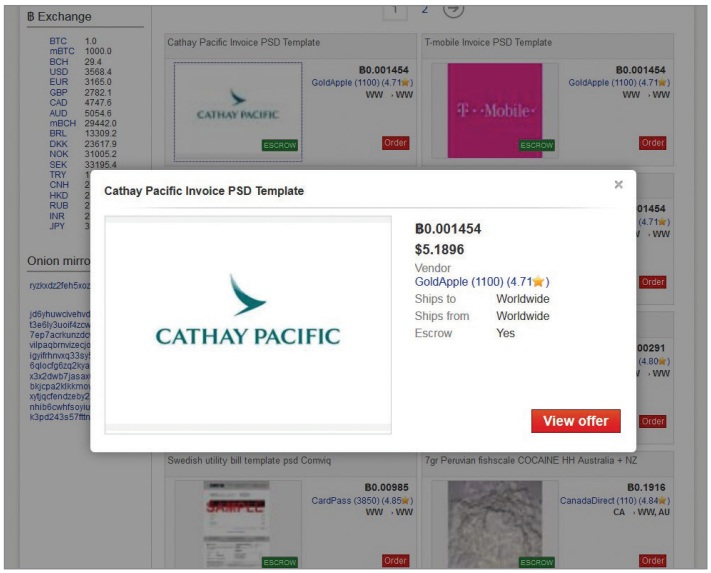

Fig.14 Fraudulent invoices for Cathay Pacific on the dark net

[35] FBI (2018)

1.5.4 TRADE SECRETS AND INTELLECTUAL PROPERTY

Data trading on the dark net is potentially the most serious where it involves the acquisition and sale of trade secrets and intellectual property. Much of this trading occurs extremely covertly, but what we do know is that it exists, and that the dark net is increasingly becoming a safe haven for it. The Enigma dark net forum (now defunct) had members who invited bids for the names of anyone who might be willing to act as an insider at enterprises that were being targeted. Information was also sought by subscribers on employees who might be available for extortion.

Our researchers performed numerous searches for still-operational platforms of this kind, but the trade seems now to have become even more covert, or to have moved to the 'invisible net' (further details of which you will find later in this report). However, one forum member we spoke to suggested that he was making good money by acting on behalf of certain clients to obtain IP and trade secrets. As a test, we provided him with the names of three leading companies and asked him what kind of espionage services could be arranged. For fees that varied from between $1,000-$15,000 he offered to obtain access to the CEO and other executive communications, or to "get whatever we wanted from their servers". Whilst there was no way of verifying these claims (short of engaging in espionage), he gave us certain information about the company that is not available in the public domain, which indicated that he might have been genuine.

2 - DARK NET ENABLEMENT OF TRADITIONAL CRIME RELATING TO THE ENTERPRISE

In addition to the more obvious threats to informational and financial security presented by the tools available on the dark net, we found a range of less obvious services which, though ostensibly more innocuous, may pose significant long-term problems for the successful running of enterprises.

2.1 - INSIDER TRADING ON THE DARK NET

As an inherently anonymous space, the dark net's hidden platforms, invitation-only forums, and private messaging systems seem ideally suited to sharing secrets about trading in stocks or attempting to gain an advantage over rival investors. We made contact with at least two individuals claiming to offer this kind of information. For example, the vendor Swag Quality was offering insider information on hedge funds and stock market trading that he claimed could be bought far more cheaply than elsewhere. However, some of the information appeared to have been acquired from a questionable Stock Market Insider platform.

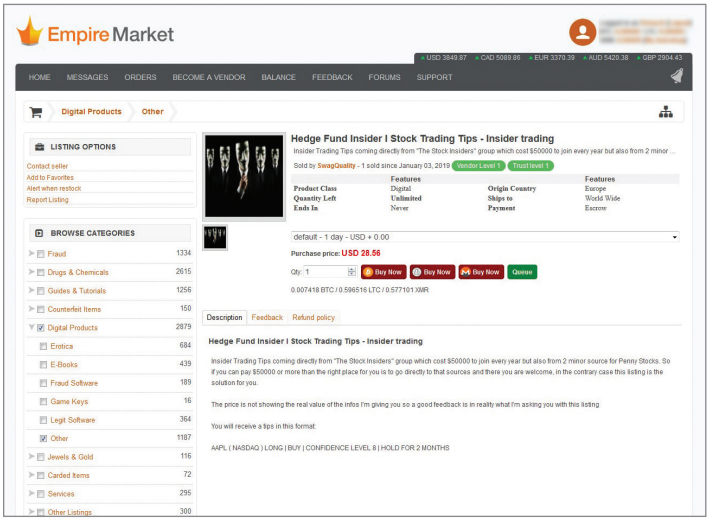

Fig.15 A vendor on the Empire Market platform is offering insider information on hedge funds

Other vendors we contacted claimed to have insider information from a variety of firms, including retailers like Tesco, along with several banks and investment firms. Thus, suspicions that insider trading is happening on the dark net are probably justified, but this is likely to be confined to more invisible locations – in particular, encrypted messaging tools, like Telegram.

2.2 - RECRUITMENT AND FRAUD

Fake credentials and identities provide a particularly buoyant market. Our research detected a wide variety of fake documentation on offer – including fake proof of employment documentation and fake college or university degree certificates from almost any leading higher education institution. A number of vendors alleged that they can help secure top posts for a variety of applicants from the executive level down to the shop floor, and even offered to hack university or previous employer databases to alter records, create fake references, and so on. See examples below:

Fig.16 Buyers can find fake degrees from almost any college or university on the dark net

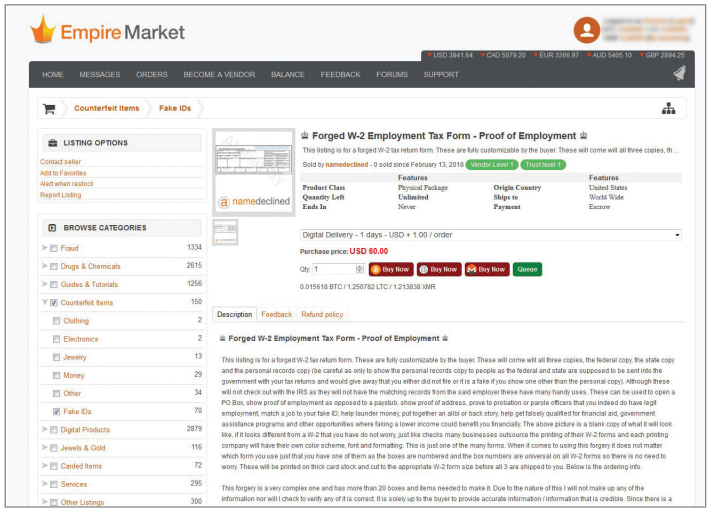

Fig.17 Forged W-2 Tax Forms are openly for sale on the dark net

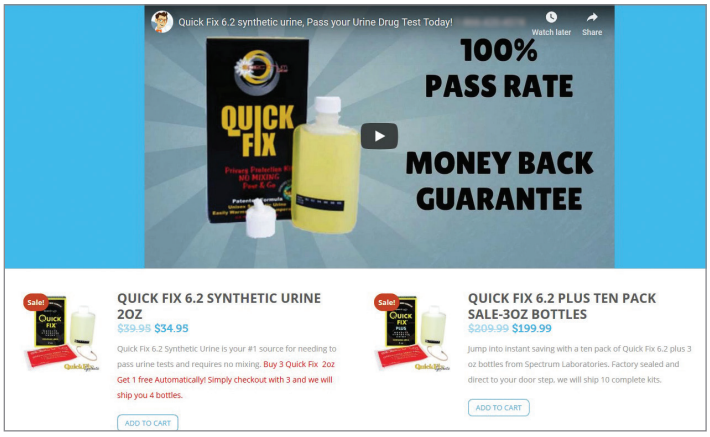

Fig.18 Quick Fix urine test kits are designed to help pass required drug tests, and often come with money-back guarantee

Services that allow employees to circumvent established safety practices (such as drug and alcohol tests) were also widely available. Many jobs like airline pilots, train drivers, bus drivers, or heavy plant equipment operators require employees to take regular drug checks. The dark net provides various tools for evading or spoofing these safety checks. We found tools to avoid detection during workplace urine testing, many of which came with money back guarantees and other marketing ploys.

3 - ENTERPRISE AND THE GREY NET: QUASI-LEGAL USES OF THE DARK NET

Just as criminals have learned how to take advantage of legal platforms like social media, businesses can unwittingly be drawn into uses of the dark net that are not always within the strict confines of the law. Identifying instances of how and when this occurs is not straightforward. Engaging in illicit or semi-licit activity too openly risks damaging an enterprise's brand and may also attract the attention of law enforcement. There are, however, enough indicators to suggest that, on occasion, enterprises are operating at the boundary of the law.

3.1 - COMPETITIVE INTELLIGENCE OR CORPORATE ESPIONAGE?

'Competitive intelligence', where companies attempt to better understand how rivals operate can easily translate to the dark net. For example, there may be useful information to acquire on the weaknesses in rivals' security, which can be used to undermine them in the market; or there may be evidence of counterfeit products, which can be used to damage the authority of a brand; or forums that can be used to test consumer opinion, or even spread negative rumours.

Posing as representatives of a mid-size enterprise in the business software sector, we contacted 20 vendors to ask whether they could use targeted penetration to provide us with the following 'items of interest to our company'. Most refused to discuss those on the forum and would only give further details once we had PM-ed them or moved to an encrypted messaging service. The breakdown of their responses is detailed below:

INFORMATION REQUESTED	NUMBER OF VENDORS REPLYING IN AFFIRMATIVE	NUMBER OF VENDORS WHO SAID THEY WOULD 'MAKE FURTHER INQUIRIES'	NUMBER WHO DIDN'T RESPOND
On product trials	10	2	8
Employee lists	14	0	6
Annual accounts	4	11	5
Directors salaries	7	5	8
CEO/executive travel plans	3	3	14

Table 6: Vendor responses to requests for corporate information

Other vendors quickly became suspicious and even aggressive when we failed to provide an initial down payment for the service. Most refused to respond to any further requests for contact, others told us (paraphrasing somewhat) to 'get off this thread if we knew what was good for us.'

3.2 - SHARING BLACKLISTS

Sharing blacklists – whether it involves rogue websites, new malware threats, or problematic customers, employees or contractors – has some obvious attractions for organisations. A recent Global Fraud survey[36] suggested that 96% of firms surveyed keep customer blacklists. Yet, fraud is not the only motivation. E-commerce retailers can often blacklist customers they consider to be disruptive. For example, several customers who bought hundreds of items from Amazon were recently blacklisted after repeatedly returning a large number of purchased items. A number of dark net vendors claimed that they could provide our researchers with lists of this kind, some for as little as $50 for up to 20,000 names and details – even though such lists contained the individuals' names, along with credit card details, and their email and mailing addresses. Knowledge of disruptive individuals is also attractive for businesses to share in order to avoid potential damage when recruiting new staff. However, this is, in many cases, illegal.

[36] MRC (2017)

4 - THE LEGITIMATE COMMERCIALISATION OF THE DARK NET BY THE ENTERPRISE

The dark net is not just a den of criminal inequity. Newer business models are now emerging where enterprises take advantage of the dark net. Legitimate commercial use of the dark net is likely to grow in the face of mounting concerns around privacy. We know, for example, that Facebook has a dark net site which is used by over a million individuals every month[37]. And there are many other legitimate uses that are becoming increasingly popular.

4.1 - CYBERSECURITY

There are certain advantages to the enterprise in being able to use the dark net for enhancing network and customer security. There is a wealth of information on dark net forums which can alert cybersecurity teams about potential vulnerabilities or emerging threats. Advanced intelligence on new hacks that are being used against them, or knowledge of tools like botnets or compromised servers, can offer enterprises significant cost savings when developing their cybersecurity methods. Active involvement in monitoring dark net activity can also be extremely useful in guarding against phishing attacks, for example, or when customer data has been breached and appears for sale on the dark net.

4.2 - SECURE COMMUNICATION

The prospect of secure communication can be attractive to news organisations who can use it to communicate with their sources. As a result, investigative reporting organisations like Propublica (https://www.propublica.org/) now have their own dark net sites. And there is also an increasing use of the dark net by other types of institutions, like the UN, which uses it to monitor activity that it shares with the police and governmental groups.

4.3 - BUSINESS INTELLIGENCE

One of the original functions of the Tor network as a government-sponsored initiative, was to ensure secure communications. As such, the dark net has arguably always been an ideal medium for the gathering and sharing of intelligence. It is hardly surprising that enterprises have also begun to see some competitive advantages in using the dark net in this way. There is a vast range of data on the dark net – so-called 'dark data' – which enterprises can use to develop customer insights, such as better understanding of consumer preferences. Dark net data can also be mined to refine operational, marketing, and new product insights. Enterprises can gather this intelligence themselves, but increasingly there is a developing industry that provides dark net information to the enterprise.

4.4 - CREDIT MONITORING

Several credit rating firms, like Experian[38], already offer services for customers to check if their details (SSN, phone number, ID info) are on the dark web. This suggests there is the potential for lenders or other credit agencies to build in extra safeguards when underwriting loans, by acquiring insights from the dark net when looking into the credit history of applicants.

4.5 - RECRUITMENT

There is also evidence that some enterprises are making use of the dark net as a tool for recruitment as it provides a novel way of reaching a community that is potentially out of reach to traditional recruitment agencies. One example was the campaign run by an anonymous organisation calling itself Cicada 3301[39], which posted a series of complex puzzles that eventually took candidates into the dark net. The identity of the organisation remains mysterious, but there are obvious precedents here for imaginative recruitment. When combined with the kind of enhanced intelligence about job candidates offered by the dark net, it seems clear that HR and job recruitment is one of many aspects of business operations likely to evolve as use of the dark net develops.

---

[37] Wong (2016)
[38] Experian Information Services: https://www.experian.com/consumer-products/free-dark-web-email-scan.html
[39] Nadel (2018)

4.6 - POTENTIAL RISKS OF ENGAGING IN THE DARK NET

Despite the potential benefits, companies should be mindful of the risks of engaging with the dark net. One is the increased risk of exposure to malware. Second, is the potential disruption to business models that have adapted to the clear net. For many companies – whether these are the giants of platform capitalism like Facebook, Twitter, and Google, or smaller, more agile businesses – there may be increased regulatory requirements that both raise costs and reduce the capacity to innovate. Worse, their traditional model of revenue generation that depends so heavily upon data collection and its commercial use is clearly at risk should anonymous commerce become an increasingly common norm.

5 - CLOSING THOUGHTS

It is clear that there is a thriving dark net market that threatens the enterprise, and solving the challenge of policing this lawless state will never be easy. We were surprised at the ready availability of services and concerned by the trend towards ever more covert operations that is taking place. While additional research is required, we were able to provide some key recommendations for both law enforcement and the enterprise to help manage the risk, which we hope will help disrupt this practice in the future and protect the enterprise.

5.1 - RECOMMENDATIONS FOR LAW ENFORCEMENT

From the perspective of law enforcement, there is a clear need to work more closely with the enterprise to identify and assist in neutralising threats from the dark net. A greater readiness to share intelligence gathered from the dark net with the enterprises will help reduce their susceptibility to certain threats – in particular, targeted attacks upon specific networks or attempts to gain control by way of remote access credentials.

The development of specialised dark net intelligence units will enhance the capacity of law enforcement to disrupt cybercriminal activity, which increasingly operates across both clear and dark nets – with one often bolstering the other. Tracking these exchanges will help reinforce the task of cybercrime prevention. Greater attention also needs to be paid to the rise of the 'invisible net', as outlined above, to ensure that the dark net does not withdraw even further into the depths. This is a significant risk, which requires further discussion and research.

5.2 - RECOMMENDATIONS FOR ENTERPRISE

For the enterprise, there is a need for greater awareness of the threats posed by the dark net in order to help build cybersecurity capacities to manage it. In particular, more attention needs to be paid to malware, such as RATs, hosted on the dark net, which allow cybercriminals to access and control corporate networks remotely. The circulation of RDPs on the dark net is also permitting cybercriminals to exert control over business networks and needs to be monitored more effectively.

The enterprise needs to expand its knowledge and understanding of the 'insider threat' to the role the dark net plays in facilitating insiders in sharing company data or assisting in breaches. Use of private or encrypted messaging systems by employees in the workplace needs to be more carefully regulated in order to restrict backdoor access for threats such as DDoS or keyloggers controlled from the dark net. This, and the prevalence of RATs, suggest that organisations must move the security perimeter down to application level and build a wall around their customer, operational, and financial data. This would secure connections to this data, even if it's being accessed by an endpoint infected by a RAT.

Enhanced training is required to educate management and staff about browser searches that redirect users to the dark net, and any use of Tor browsers in the workplace needs to be more carefully monitored. Yet, greater protection for users also needs to be in-built. Virtualisation

technology that isolates threats can help here by rendering malware harmless. Employees no longer have to be the last line of defence, and can open email attachments or click on websites without fear of picking up malware.

Greater care is also required to prevent sensitive operational details – in particular, corporate email chains – from being stolen and sold on the dark net. In general, content of business emails should be more carefully regulated, and more robust policies should be developed around the inclusion of sensitive content, such as passwords or financial information.

Also, the increase in recruitment-related fraud involving falsified credentials that can be easily obtained on the dark net should be more closely monitored. Typical items enterprises should be on guard against include fake college diplomas, doctored CVs, and counterfeit passports.

However, threats posed by the dark net should not limit the business opportunities it can offer. These include access to a wider, more diverse customer base, more innovative marketing methods, and new ways of building client trust by enhancing anonymity. Enterprises should be prepared to develop resources for using the dark net to their advantage.

In particular, capacity should be built around enhanced use of the dark net for intelligence and cybersecurity purposes. This includes monitoring dark net marketplaces for malware involved in compromises of enterprise networks, watching for company or customer data being traded there, and checks on potential misuse of the company brand for the purposes of phishing or reputational attacks, such as the sale of spoof webpages or company invoices. Regular monitoring could also assist in preventing unfettered trading in company IP or in counterfeit versions of its goods. However, expert advice should always be sought to ensure that dark net activity is compliant with current regulatory frameworks and the law.

METHODOLOGY

RESEARCH METHODOLOGY

For the purpose of this research, we conducted an analysis of 15 leading dark net platforms during the period of November 2018 to March 2019. During this period, more than 70,000 listings were examined across these platforms, and a variety of aspects, such as commodities sold, prices, vendor responses, and patterns of trading, were scrutinised. Membership was obtained to three forums attached to these platforms, in order to engage in observation, intelligence gathering, covert yet simulated transactions, and other ways of gathering data. In addition, qualitative interviews were conducted with 30 vendors either as part of responses to ads, or in the course of simulated purchases. A threat assessment tool was also developed to better evaluate the multidimensional nature of threats posed to the enterprise by dark net tools and services.

The research utilised a mixed methods approach which used three types of metrics.

(i) Platforms studied included:

- **Dream Market**
- **Empire Market**
- **Wall Street Market**
- **Agora**
- **darkOde**
- **Point/T-chka Free Market**
- **Olympus Market**
- **Ramp (Russian Anonymous Market Place)**
- **RuTor**
- **Silk road 3**
- **Deep Sea**
- **Berlusconi Market**
- **IDC**
- **Wayaway**
- **ToyouTeam**

(ii) Covert observations and discussions on three forums, Empire Market, Dream Market and The Hub, to gather intelligence by discussion, questioning, and engaging in simulated transactions.

(iii) Qualitative interviews with 30 vendors either as part of responses to ads, or in the course of simulated purchases.

A variety of primary and secondary sources were also consulted to enhance the evidence base.

METHODOLOGY
CONTINUED

METHODOLOGY FOR DEVELOPING DARK NET THREAT ASSESSMENT TOOL

To analyse data and the threat presented by dark net activity to the enterprise, we developed a 3D dark net threat assessment tool. Twelve categories of potential threat were defined (indicated in the table below). A panel of six experts in cybersecurity, cybercrime, law enforcement and business management were then consulted and asked to use their knowledge and experience to evaluate the threat to the enterprise posed by dark net commodities from within each category. 'Threat' was defined in terms of three key metrics whereby harm to an enterprise might occur:

Disruption – ways in which dark net tools or services might undermine the everyday functioning of a business

Devaluing – ways in which dark net tools or services might help erode the market of a business; for example, by handing advantage to a competitor or undermining trust in the brand

Defrauding – ways in which dark net tools or services might involve financial loss

Threats were evaluated on a scale of one to 10 for each, producing a possible total score of **30** across each category. Scores were then correlated with threat levels as follows:

20 – 30: high threat level

10 – 19: medium threat level

0 – 9: low threat level

	CATEGORY	3D THREAT SCORE	THREAT LEVEL
Network compromises			
1	Infection / attack tools	**22**	**High**
2	Access	**27**	**High**
3	Targeting and espionage	**26**	**High**
4	Support services	**18**	**Medium**
Financial attacks			
5	Credentials	**28**	**High**
6	Phishing tools	**28**	**High**
7	Refunds and other scams	**19**	**Medium**
Data theft			
8	Customer data	**25**	**High**
9	Operational data	**17**	**Medium**
10	Financial data	**23**	**High**
11	Trade secrets and IP	**16**	**Medium**
Other			
12	Emerging threats	**20**	**High**

Table 7: 3D threat scores for each category examined

METHODOLOGY
CONTINUED

	DISRUPTION	DEVALUING	DEFRAUDING	TOTAL
Network Compromise				
Infection/attack tools	10	7	5	**22**
Access	10	9	8	**27**
Targeting and espionage	9	8	9	**26**
Support services	6	5	7	**18**
Financial Attacks				
Credentials	8	10	10	**28**
Phishing tools	8	10	10	**28**
Refunds and other scams	5	6	8	**19**
Data Theft				
Customer data	8	9	8	**25**
Operational data	6	6	5	**17**
Financial data	7	8	8	**23**
Trade secrets and IP	5	7	4	**16**
Other				
Emerging threats	7	6	7	**20**

Table 8: Breakdown of 3D threat scores for each category

BIBLIOGRAPHY

Allen, P. (2018) Half of data breaches are the fault of insiders, not hackers, research finds, Computing 01/10/2018

Branwen (2019) Darknet Market Archives (2013-2015), https://www.gwern.net/DNM-archives

Brignall, M. (2016) Banned by Amazon for returning faulty goods, The Guardian, 18/03/2016

Casal, J. (2017) 1.4 Billion Clear Text Credentials Discovered in a Single Database, Medium, 09/12/2017

Chargebacks (2019) Chargeback Stats, 08/02/2019

Christin, N. (2017) An EU-focused analysis of drug supply on the AlphaBay marketplace, EMCDDA, 11/2017

Cimpanu, C. (2019) Authorities shut down xDedic marketplace for buying hacked servers, ZDnet, 28/01/2019

Darkweb News (2017) Nuke Malware For Sale on the Dark Web, 10/08/2017

Denton, D. (2017) Annual sales estimation of a darknet market, Denton, 25/05/2017

Equifax (2018) How financial crimes are hidden in the dark web, Knowledge Centre (Identity Protection), 2018

Europol (2019) Double Blow to Dark Net Marketplaces, 2019

Experian (2018), Is your information on the Dark Web?, 2018

FBI (2018) Business E-mail Compromise The 12 Billion Dollar Scam, Public Alert Number I-071218-PSA

FDA (2018) FDA launches global operation to crack down on websites selling illegal, potentially dangerous drugs, US Food and Drugs Administration, Press Release, 23/10/2018

Fearn, N. (2018) BT starts sharing malware data with rival ISPs in 'world's first', The Inquirer, 07/02/2018

Filecloud (2018) The Biggest Threats from the Dark Web That Keep Businesses on Their Toes, Security 07/09/2018

Hazlehurst, B. (2016) Meet New Zealand's 19-Year-Old Jordan Belfort Getting Rich Racketeering on the Dark Web, Vice, 13/10/2016

Hoyme, C. (2018) The Dark Web and its Impact on Small Business, Jackson Lewis Workplace Privacy, Data Management & Security Report, 21/02/2016

Iiascu, I (2019) Banks in West Africa Hit with Off-The-Shelf Malware, Free Tools, Bleeping Computer, 17/01/2019

Infosec (2018) Malware in Dark Web, 15/01/2018

IntSights (2018) Financial Services Threat Landscape Report, 07/2018

Ismail, N. 2018 The financial impact of data breaches is just the beginning, Information Age 8/01/2018

Kahn, R. (2018) Economic Espionage in 2017 and Beyond: 10 Shocking Ways They Are Stealing Your Intellectual Property and Corporate Mojo, Business Law Today, ABA, 19/09/2018

Kelion, L. (2017) Dark web markets boom after AlphaBay and Hansa busts, BBC, 01/08/2017

Kinder (2017), T. Hedge funds turn to dark web to gain an edge, Financial News, 02/08/2017

Krebs, B. (2015) Bidding for Breaches, Redefining Targeted Attacks, Krebs on Security, 15/09/2015

Lublin, J. (2010) How a Black Mark Can Derail a Job Search, Wall Street Journal, 02/02/2010

BIBLIOGRAPHY
CONTINUED

Migliano, S (2018) Dark Web Market Price Index: Hacking Tools (US July 2018 Edition), 30/07/2018

MRC (2017) Global Fraud Survey, Merchant Risk Council, 07/2017

Munro, D. (2016) Healthcare's Latest Cyber Threat: Source Code For Sale On The Dark Web, Forbes, 16/08/2016

Nadel, D. (2018) Puzzling the Internet: The Mystery of Cicada 3301, Turbofuture, 14/07/2018

Ng, A. (2018) FBI nabs hackers in theft of 15m credit cards from Chipotle, others, CNet, 01/08/2018

Nicholls, S. (2018) Police spies helped create employee 'blacklist' for UK companies, force admits, Euronews, 24/03/218

O'Flaherty, K. (2019) Another 127 Million Records Have Gone On Sale On The Dark Web -- Here's What You Should Do, Forbes, 15/02/2019

Oh, S. (2018) Why is the U.S. accusing China of stealing intellectual property?, Marketwatch, 06/04/2018

Paganini, P. (2017) MACSPY – Remote Access Trojan as a service on Dark web, Security Affairs, 14/06/2017

Palmer, D. (2018) This dark web market is dedicated to compromising your emails, ZDNet, 05/10/2018

Preston, W. (2019) Protecting Corporate Data…When an Employee Leaves, Druva Blog, 24/01/19

Proofpoint (2018) Drive-by as a service: BlackTDS, 13/03/2018

Raeburn, S. (2013) LinkedIn SWAM 'blacklist' censoring legitimate users, critics claim, The Drum, 21/08/2013

Rempfer, K. (2018) Air Force drone, Army tank documents for sale on dark web, Airforce Times, 11/07/2018

Repknight (2018) Securing the Law Firm: Dark Web footprint analysis of 500 UK legal firms, White paper, 01/2018

Schlesinger, J. & Day, A. (2018) Hackers are selling access to law firm secrets on dark web sites, CNBC, 12/07/2018

Schwartz, M. (2018) Cybercrime Markets Sell Access to Hacked Sites, Databases, Bank Info Security, 21/09/2018

Seqrite (2017) Seqrite Cyber Intelligence Labs reports breach at IRINN affecting over 6000 Indian organizations, 03/10/2017

Singh, S. (2017) Market manipulators hook onto dark web, private chats for stock tips, Times of India, 26/11/2017

Soska and Christin (2015) Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem, available at: https://www.usenix.org/system/files/conference/usenixsecurity15/sec15-paper-soska-updated.pdf

Spencer, L. (2017) Govt calls in the feds over dark web Medicare data claims, ARN, 04/07/2017

Trend Micro (2017) Access to Corporate Remote Desktops Sold for $3 in the Dark Web, Security News, 07/11/2017

UK Finance 2019a, Business Payments Survey 2019

UK Finance 2019b, Fraud the Facts 2019

BIBLIOGRAPHY
CONTINUED

US IP Commission (2017) Update to the IP Commission Report, Commission on the Theft of American Intellectual Property

Vigliarolo, B. (2018) How to protect yourself from the Telegram-exploiting remote access Android HeroRat Trojan, TechRepublic, 02/07/2018

Wiat, A. (2018) A new generation of phishing tools was discovered In Darknet, CWIS, 02/05/2018

Wong, J. (2016) A million people now access Facebook on the “dark web” every month, 22/04/2016

Zorz, M. (2018) Access to airport’s security system sold on dark web, HelpNet Security, 11/07/2018

Bromium, Inc.
20883 Stevens Creek Blvd.
Suite 100
Cupertino, CA 95014
+1 408 213 5668

Bromium UK Ltd.
2nd Floor, Lockton House
Clarendon Road
Cambridge CB2 8FH
+44 1223 314914

For more information
visit Bromium.com or write to
info@bromium.com.