INTO THE WEB OF PROFIT

SOCIAL MEDIA PLATFORMS AND THE CYBERCRIME ECONOMY

The next chapter of *Into The Web of Profit*

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

Sponsored by Bromium

Br Bromium®

FOREWORD

GREGORY WEBB,
CEO of Bromium

When we started working with Dr. McGuire, we wanted to highlight the social impact that cybercrime is having on the world today. His research findings were startling. The original "Into the Web of Profit" report showed that the cybercrime economy was generating $1.5 trillion in revenue each year, with some of the funds being rediverted back into traditional crimes, such as human trafficking and terrorism.

One of the most interesting outcomes of the report was the identification of a new form of cyber-enabled crime – platform criminality. Platform criminality mirrors the disruptive platform-based business models popularised by the likes of Uber and Amazon, with data as its key commodity. The results were shocking, and are still being discussed within government, law enforcement and business today. So much so, we felt that further investigation was needed.

In this next chapter, we take a closer look at the clear web, investigating the role of popular social media platforms in cybercrime and other forms of crime-enablement. The findings show that the problem is perhaps even worse than we thought and should act as a wake-up call not just for law enforcement and governments, but also individuals and businesses.

Social media has been a thorn in the side of enterprise security for some time now. Up to 1 in 5 businesses have been infected with malware originating from social media and 1 in 8 have experienced a security breach as a result of a social media-directed cyberattack. While in the early days, companies tried to ban its use, social media has become such a powerful tool for enterprise – particularly for marketing and HR – that preventing its use is simply not practical.

This report shows that social media is a huge blindspot in enterprise defences. It is enabling rapid infection across huge user bases, as well as providing easy access to would-be hackers to get the tools and services they need to launch attacks. Quite frankly, it's worrying. This backdoor access to enterprise systems is putting customer data and business IP at risk on a daily basis. And, at the moment, enterprises and individuals are simply not geared up to deal with it.

Reading this report should make every business ask themselves: How am I defending my organisation against social media-enabled attacks? My three key takeaways are:

1. Social media platforms are being used as a trojan horse by hackers to enter the enterprise. Cybercriminals can use simple hacks to reach millions of users, globally, with very little effort on their part: social media is in effect a global distribution centre for malware. One in five organisations have now been infected with malware distributed via social media. Research conducted for this report found up to 40% of malware infections identified were connected to malvertising. A further 30% came from malicious plug-ins and apps. Employees casually clicking on malicious content spread by cybercriminals are unwittingly acting as trojan horses, giving hackers backdoor access to high value assets.

2. Social media is enabling the spread of cryptomining malware. Data obtained through this research shows that four of the top five global websites hosting cryptomining code are social media platforms. Something as innocuous as clicking on a YouTube advert can result in cryptomining malware installing onto devices and hijacking them to mine cryptocurrentcy, increasing power consumption, and potentially using cryptojacking payloads for even more nefarious purposes in the future. The brilliance of this – from a hackers' perspective – is that a lot of victims won't even know they have been hit, meaning that hackers can go undetected for a long time. But the increased performance strain on the CPU or GPU will accelerate the deterioration of enterprise equipment and drain IT resources, causing significant rising costs in relation to computing power.

3. Social media is making it even easier for would-be attackers to get the tools and expertise they need to launch their assaults. The report found widespread availability of hacking services, hacking tutorials and the tools needed to aid hacking efforts, like exploits and botnet hire. The boundary between social platforms and Dark Web equivalents is becoming blurred, with tools and services freely available, or acting as an entry point for more extensive shopping facilities on the Dark Web.

Ultimately, hackers know your weak spot – your employees – and they know how to manipulate them through trusted connections. Cybercriminals know that they likely won't get caught. It's a numbers game. And social media puts the odds of finding someone who will click on their malware firmly in cybercriminals' favour. Only with a thorough understanding of the scope of the problem and deploying advanced capabilities, including containment, to defend ourselves can we start to tip the balance. If we carry on as we are, then we are just sitting ducks.

CONTENTS

EXECUTIVE SUMMARY

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

Cybercrime does not remain static for long. Opportunities constantly arise from technical and social innovations, with hackers finding new ways to exploit the latest browsers, ecommerce sites or mobile computing devices. It is no different for social media. The power of social media platforms is based upon their capacity to connect users in new ways and create new avenues for interaction. For individuals, enterprises and governments, they facilitate new pathways for reaching an audience, promoting a product and fostering communities.

Social media platforms are equally attractive to cybercriminals. Yet the growing range of criminal risks encountered across social media remains significantly under-researched. This report outlines how the sharing of malware, or the buying and selling of services, tools and data on social media platforms, is contributing to cybercriminal opportunities and furthering traditional crime. It also highlights the impact this is having on users and organisations, showing how:

- Social media platforms have created an attractive opportunity for cybercriminals for revenue generation within the clear web – often as much, or more, than can be made via more traditional illicit channels like the Dark Web.
- The vast user base and unique levels of trust on the part of the social media users are facilitating swift and far-reaching dissemination of malware that can infect individuals, organisations and whole nations.
- The very nature of interaction between users on social media promotes ‘chain exploitation’ – rapid and seamless spread of infection rates, offering cybercriminals a toolbox of very effective attack methods.
- Attacks are being tailored to specific platforms, with characteristics of social networks being deployed against users like weapons – like LinkedIn’s ‘confirm that you know’ feature.
- The lines between legitimate social media platforms and their equivalents on the Dark Web are becoming blurred, with some platforms being used as a marketing resource to advertise cybercriminal tools and services or acting as a shop window for more extensive facilities on the Dark Web.
- Cybercriminals are exploiting social media platforms for more traditional forms of offline crime – such as the recruitment of millennial money mules to aid in money laundering and the sale of drugs.

This report aims to provide a thorough understanding of the scale of crime being committed on social media platforms, offering the insight needed to help disrupt the Web of Profit.

THE STORY IN STATISTICS

From the available evidence it is clear there are some striking trends in the use of social media platforms in crime:

- This research calculated that social media-enabled crimes are generating global revenues of at least **$3.25bn** for the global cybercrime economy annually
- Data obtained from the ICC for this report shows reported crimes involving social media grew more than **300-fold** between 2015-2017 in the US, while UK police data shows social media-enabled crime **quadrupled** between 2013 and 2018
- Web of Profit researchers calculated that over **1.3 billion** social media users have had their data compromised within the last five years and between **45-50%** of the illicit trading of data from 2017 to 2018 could be associated with breaches of social media platforms, like LinkedIn and Facebook
- This research found that social media platforms contain up to **20%** more methods by which malware can be delivered to users – e.g. through updates or shares, add-ons, plug-ins etc. – than comparable sources, such as ecommerce, media or culture-orientated websites
- Around **30-40%** of social media infections come from infected ads
- At least **20%** of social media infections arise from add-ons or plug-ins for social media platforms
- Social media has become a key pathway for cryptomining software. Up to **1 in every 500** of the most searched-for websites are estimated to carry such software, with social media occupying **4 out of the top 5 slots**
- Around **30-40%** of the social media platforms inspected for this report had accounts offering some form of hacking service
- Our research found offers for botnet and booter hires on Facebook, Instagram, Twitter and several other sites. Prices were fairly stable, with an average cost of around $10 for a month or $25 for a lifetime rental
- Criminal revenues from fraud enabled by social media have increased by over **60%** since 2017
- Data obtained during this research from CIFAS shows that since 2016, there has been a **36%** rise in the use of social media platforms to recruit money mules under the age of 21

1.1 SOCIAL MEDIA PLATFORMS AND THE CYBERCRIME ECONOMY

Most available research attempts to estimate the value of cybercrime based on its costs – the amount of damage that breaches and data theft cost corporations. A better approach would be to look at revenues generated from cybercriminal activities – it explains the motivation for engaging in such crime and helps track (and possibly disrupt) criminal activity, as highlighted in *'Into the Web of Profit'*.

Criminal platforms on the Dark Web are direct revenue generators, but the extensive use of legitimate platforms for criminal purposes offer a further revenue stream. This raises an important question about the social media platforms considered in this report – what kind of contribution to this cybercrime economy are they creating? We can make educated, albeit provisional, estimates – especially if these are kept as conservative as possible and based only upon what we know, rather than what we think we know. Using just four indicators, it was possible to derive the following estimates[1]:

> *"Criminal platforms on the Dark Web are direct revenue generators, but the extensive use of legitimate platforms for criminal purposes offer a further revenue stream.*

Figures calculated as part of this investigation show social media platforms contribute at least **c. $3.25bn** annually to the global cybercrime economy. This is based on the following areas:

- Illegal pharmaceutical sales (i.e. prescription drugs) – **$1.9bn**
- Stolen data sales – **$630m**
- Financial fraud – **$290m**
- Cryptomining malware – **$250m**
- Romance/dating fraud – **$138m**

However, in addition to these sources of 'direct' revenue, cybercriminals have many other ways to use social media for revenue generation, such as malware and hacking services, intellectual copyright theft involving fake brands and illegal drug sales (such as cocaine, MDMA and heroin), to name a few. Revenues from these activities have not been included in the above estimate since available data is not robust enough to permit us to make any kind of reliable inferences. It is, however, safe to assume that the total level of criminal revenues from social media is likely to be much higher.

> *"In the information economy, data has become the newest form of commodity exchange.*

1.2 SOCIAL MEDIA PLATFORMS: A RICH TARGET FOR CYBERCRIMINALS AND A HAVEN FOR HACKERS

In the information economy, data has become the newest form of commodity exchange. Social media platforms' ceaseless focus on the acquisition of personal data has turned them into data banks that are highly attractive to cybercriminals. Whether it is the size of user base, the type of data exchanged, or the high levels of user trust engendered, social media platforms are one of the new 'go-to' targets for hackers seeking data.

There is growing evidence that social media users and their data are becoming significant resources that can be exploited by cybercriminals. In fact, this investigation found over **1.3 billion**[2] social media users have had their data compromised within the last five years, and between **45-50%** of data being traded online could be associated with data obtained through social media data breaches.[3]

[1] Details of the calculation can be found in the methodology section of this report, Appendix 1.

[2] Details of the calculation can be found in the methodology section of this report, Appendix 1.

[3] This finding is corroborated by indicators from within Gemaltos Breach Level index, a global database of public data breaches, which suggests that social media breaches accounted for over 56 percent of the total records compromised in the first half of 2018. Only six social media breaches, including the Cambridge Analytica-Facebook incident, were responsible for hundreds of millions of records being stolen, showing just how severe the consequences of social media data theft can be.

Research shows that employees can spend over three hours per working week browsing social media sites.

Social media platforms are offering an easy route for hackers to reach or research their selected targets. FBI data has suggested a **300-fold** rise in reports of crimes involving social media between 2015-2017.[4] This striking increase is no doubt partly explained by the greater likelihood of victims reporting such crime or law enforcement categorising it in this way. Nonetheless, significant rises are corroborated in other, more localised, police data, with some forces reporting that social media-enabled crime **quadrupled** between 2013-2018.[5]

Worryingly for businesses, research shows that employees can spend over three hours per working week browsing social media sites. The same research showed up to 77% of employees say they use social media in the workplace, regardless of whether there are policies in place for how this should be used.[6] Business itself is equally implicated in the growing dependence upon social media platforms. It has been estimated that circa 73% of businesses use a Facebook account for work purposes, 64% use LinkedIn and 56% use Twitter.[7] It is no surprise that more than 1 in 5 businesses have been infected with malware as a result of direct contact with social media platforms.[8]

1.3 SOCIAL MEDIA PLATFORMS AS MALWARE DISTRIBUTION CENTRES

The sheer number of social media users worldwide means that social media platforms have become one of the major sources for malware infection online, for both individuals and organisations. The problem is growing. Social media platforms contain up to 20% more methods for potential malware delivery than comparable sources, such as ecommerce, media or culture-orientated websites.[9] This is because they generally contain more images, videos, adverts and plug-ins. Platform-specific threats like Facebook scams have been rated as the number one method for compromising an enterprise network[10], with some sources claiming that as many as **1 in 8** have experienced a security breach resulting from a social media-directed cyberattack.[11]

1 in 8 businesses have experienced a security breach resulting from a social media-directed cyberattack.

The spread of malware is not just facilitated by the large user bases of social media, but by factors such as the greater sense of trust users feel when clicking on suspect links and the structural phenomenon of 'chain exploitation'.[12] Here, the very nature of interaction across social networks promotes rapid and seamless spread of infection – a problem made vastly more complicated by the tendency for social media to allow user profiles to be shared across multiple platforms. One typical example of this kind was phishing links on Facebook Messenger that were used to connect victims to a site resembling YouTube. After downloading an update, users were then infected with sophisticated malware able to steal passwords, and more.[13]

[4] (FBI 2015-2017). In 2015, 58 reports relating to social media being used as a medium or a tool to facilitate a cybercrime were received. By 2017 the number was 19,986.

[5] Facebook figured most often in this data, being involved in nearly five times as many reports involving crime as the next highest platform. Snapchat exhibited one of the highest rates of increase in reported crime – more than 1,000% higher than the next highest, Instagram. (Reynolds 2018)

[6] Bean (2017), Pew (2016)

[7] Osterman (2016)

[8] Cimpanu, 2018

[9] Extrapolated from an analysis of 10,000 malware infection types and their sources.

[10] Cisco (2015)

[11] Hayes (2016)

[12] Aditya and Enbody (2011)

[13] Palmer (2018)

2.1 AMPLIFICATION, PERSUASION & CONTAGION

> *Cybercriminals are becoming accomplished at building upon the amplificatory power of social media to develop ways of engaging their victims.*

Chain exploitation and its power in enabling cybercrime can be associated with three key features of social media that cybercriminals are learning to exploit:

1. AMPLIFICATION

In a world where two-thirds of American adults get their news from social media[14], social platforms now provide the most obvious available springboard for disseminating social engineering strategies. Indeed, by placing almost anything on social media platforms – whether that be commercial products, fake news or political messages – the reach is amplified to produce what is often an exponential expansion of an individuals' networks of influence.

2. PERSUASION

'Talking louder' may reach more ears, but it doesn't guarantee the message will get across. By its very nature, social media is a domain where popularity is a highly valued currency. Marketers now routinely distinguish between two versions of amplification – *'reach'* (the number of unique individuals who view a page) and *'impressions'* (the total number of times content is displayed to people). But social media campaigns are also concerned with *'engagement'* – the extent to which individuals respond to content. For example, by liking, commenting or posting further content. Cybercriminals have learned these lessons and are becoming far more accomplished at building upon the amplificatory power of social media to develop ways of *engaging* their victims – that is, to catch their attention and make them more malleable to exploitation. In fact, they appear to be much better than marketers at engagement given that they are so often successful at transforming mere engagement into *persuasion*. For example, by persuading victims to not only look at 'interesting' apps but to follow them or download content.

> *Up to 70% of successful ransomware attacks originated from phishing links via emails or social media platforms.*

Social media users appear to be highly susceptible to persuasion, with recent psychological research suggesting that habitual users of social media platforms like Facebook are up to 40% more likely to click on links that lead to phishing or spam-based infections than infrequent or non-users. Regular users are also more likely to respond to friend-based attacks (i.e. to click on links in messages from 'friends') compared to infrequent visitors to social media sites or non-users.[15]

Persuasion is clearly more profitable for cybercriminals than engagement, in that it can result in directing behaviour or opinion beyond the immediate confines of a platform — in everything from changing voting intentions, or agreeing to act as a money mule.

3. CONTAGION

The phrase 'gone viral' is now a common term of reference when discussing an idea or trend that suddenly acquired huge popularity. However, its origins within cybercriminality are perhaps not as well appreciated as they should be. The computer virus is the archetypical example of how content can spread extremely rapidly, often exponentially, through a given medium. It should be no surprise then that contemporary platform-focused cybercriminals are just as aware as marketers that once a certain tipping point in the cycle of amplification and persuasion is reached, they will be able to reap significantly more benefits from an illicit endeavour.

Amplifying a scam until it becomes all but omnipresent is a kind of holy grail for cybercriminals. Now, cybercriminals have spotted the potential of social media contagion in enhancing revenue generating initiatives. For example, up to 70% of ransomware attacks that were successful in 2017 originated from phishing attacks via emails or social media platforms. Worryingly for business, most of these social media-enabled ransomware attacks were directed at enterprise networks.[16]

[14] Pew (2017)

[15] Halevi et al (2013), Vishwanath (2015)

[16] Jay (2018)

Some of the most familiar cyber scams have involved contagion-oriented strategies. Mass marketing frauds like old fashioned 419 scams are one example, as is the mass distribution of spam. More recently, social media has proved to be susceptible to attacks that use fake advertisements or thematic finance-based hashtags targeted at individuals who have exhibited a preference for certain financial institutions.

3.1 COMMON ATTACK METHODS ON SOCIAL MEDIA

Some of the most common methods and techniques identified as part of this research to exploit the social media ecosystem and spread infections include:

Infected adverts – around **30-40%** of social media malware arise from clicks on infected adverts. Notorious examples of this include adverts for Ray-Ban sunglasses or Nike shoes found on Instagram, Facebook and elsewhere, which deliver a virus when clicked.[17]

Plug-ins and apps – this report found that at least **30%** of social media infections arise from social media plug-ins that claim to provide additional functionality for victims. These include games, personality tests and more. The volume appears to vary significantly by platform. For example, at least **60%** of infections on Facebook arise from malicious 3rd party apps downloaded from the site.

News posts, updates and photos from friends – receiving updates about what friends are doing or what is happening in the wider world has been an obvious ingredient of the appeal of social media. Cybercriminals have been quick to see how posts or updates from friends can be exploited to plant malware or to access personal data. The extensive use of friends' and associates' photographs across the Facebook platform has provided another risk. Cybercriminals have used photo tag notifications to persuade users to open an attachment, which then downloads malware.[18]

Funny photographs and videos – another method of criminal persuasion utilises links to the 'funny' or amusing videos often found in social media posts. Around **15%** of social media infections come from this method and in 2015, over 100,000 Facebook users were infected over the course of just three days in this way. [19]

Drive-by downloads – these are malware downloads which can happen even when the user doesn't actively open any files or install content. Even a seemingly innocuous action, like visiting a website recommended in a social media post can be risky if the website has been hijacked and contains a small piece of code which redirects the user to another address containing malware. The wide variety of content that can be accessed via social media platforms make users especially vulnerable to such attacks. Data obtained for this research from SANS shows that drive-by download attacks now represent one of the common methods used by cybercriminals to attack organisations, accounting for around 48% of attacks which exploit Web-based vulnerabilities.[20]

Phishing and spear phishing – there has been a rise of 'social network phishing', where cybercriminals create fake social media pages for data harvesting. In 2018, **60%** of social network phishing occurred via fake **Facebook** sites, **20%** via fake sites for the Russian social media platform VK and around **13%** via phony **LinkedIn** pages. Social media phishing has been estimated to have near doubled in 2017[21] and the capacity of hackers to persuade social media users to access infected links is greatly aided by spear phishing techniques, which use personalised details of posts and topics obtained from timelines to make the victim believe a connection is real. Recent research has suggested anything between a 30-60% success rate in persuading users to click on more personalised content.[22]

[17] Krustev (2018)
[8] Pesce et al (2012)
[19] Ragan (2015)
[20] SANS (2017)
[21] Barker (2018)
[22] Seymour & Tully (2016)

3.2 TAILORING ATTACKS TO SPECIFIC SOCIAL PLATFORMS

Not only can platforms be distinguished by the specific kinds of services they offer, but also by their distinct design and functionality. Cybercriminals are adept at tailoring their activities to the specific features of each platform they misuse:

- **Facebook** has proved to be an obvious resource here, constituting one of the top 3 targets for phishing attacks in 2017 – a clear indication of cybercriminals' awareness of the amplificatory power of social media as a silo for acquiring personal data.[23]
- **LinkedIn** is based on the capacity to add others to your professional networks – a fundamental feature that cybercriminals have learned to exploit. Fake 'confirm that you know' emails are almost indistinguishable from genuine emails and have been found to redirect users to malicious sites where malware is downloaded. Up to 68% of LinkedIn users who receive such emails have been found to click on the link, enabling cybercriminals to identity key individuals within an enterprise and acquire their login details and more.[24] Cybercriminals are also accomplished at exploiting the way LinkedIn ranks relationships on three levels – first, second, and third-degree connections. Since first degree connections are perceived as being the most trustworthy, they are attractive tools to use for phishing attacks or malware dissemination. The dependence of LinkedIn upon contacts built across online networks, rather than by direct social acquaintance, is a further factor in enabling infections to spread more rapidly.[25]

> *“Up to 68% of LinkedIn users who received fake emails asking them to confirm their connection to other individuals, have been found to click on phishing links.*

- **WhatsApp's** capacity for voice messaging, sharing links, forming groups, etc. lends itself to distinctive attack methods. For example, WhatsApp messages were distributed with links offering a premium 'upgraded' version of WhatsApp, called 'WhatsApp Gold'.[26] The new premium service offered a range of features not available to standard users, such as instant message deletion or the opportunity for talking directly with celebrity users of the app. When downloaded, software which monitored user's activity - including listening in on conversations – was installed.[27]
- **YouTube** videos often suggest or even require the user to click through to the suggested link. Cybercriminals have been exploiting this feature to launch attacks related to popular games. For example, Fortnite players were offered free in-game currency, however upon clicking on provided links, users were redirected to an external site, pushing malware to be downloaded on their devices.[28]
- **Instagram** users' comments on posts have proved to be a fertile source of illicit revenue. In one case, comments on Britney Spears' Instagram page redirected traffic to the command and control page for the Turla cybercrime group. A backdoor piece of malware was then installed to gather information on the user.[29] In another example, 13 Instagram credential-stealing apps were detected on Google Play. These apps, supposedly designed to manage or boost followers, were intended to acquire Instagram credentials. Once credentials were stolen, the hackers were able to use them to send out spam and ads from the account, with up to 1.5 million users potentially installing the apps.[30]

[23] Kaspersky (2018)
[24] Boodai (2011)
[25] Tsing (2018)
[26] Action Fraud (2019)
[27] Correa (2016)
[28] https://www.polygon.com/2018/5/4/17307268/fornite-scams-youtube-free-v-bucks
[29] Matthews (2017)
[30] Leyden (2017)

4.1 EMERGING THREATS TO SOCIAL MEDIA USERS AND THE BUSINESSES THAT EMPLOY THEM

DIGITAL CURRENCY AND CRYPTOCURRENCY SCAMS

Social media platforms have become increasingly important to the business of digital currency and cryptocurrency scams. Data obtained from UK police during this investigation found 203 incidents of cybercriminals using social media platforms to advertise fraudulent investments involving cryptocurrency trading and mining between June and July 2018. They estimated the victims incurred losses of around £2m ($2.5m).[31] In 2018, at least 80% of initial coin offerings (ICOs) were scams,[32] and social media has played a significant role in enabling these. For example, at least 15,000 bots pushing cryptocurrency scams have recently been detected on Twitter.[33]

Another example involves the hijacking of trustworthy verified accounts, like the UK retailer Matalan, which was changed to resemble Elon Musk's personal profile. Tweets were then sent out from the fake 'Elon Musk' account asking for a small Bitcoin donation – with a promise of bitcoin 'rewards'. The scam was made more credible by including responding tweets from other 'trustworthy accounts' saying they had received the reward after their donation. Needless to say, no-one who donated received anything in return.[34]

> *Social media platforms have become increasingly important to the business of digital currency and cryptocurrency scams.*

CRYPTOJACKING

The rise of 'cryptojacking' and 'cryptomining' malware is an increasing concern for social media users and businesses in particular. The process of generating revenues by cryptomining requires a computer to perform complex calculations to generate new cryptocurrency – but this process takes up a lot of memory and processing time. Criminals hijack other computers to perform the task, thereby passing computing costs on to an unsuspecting third party.

There has been a 400-600% increase in illicit cryptocurrency mining malware detections globally since 2017.[35] The majority of illicit cryptocurrency malware detected as part of this investigation appeared to be directed towards Monero (around 75-80% detected) and Bitcoin (10%).[36]

This effort means that cybercriminals may be earning close to a quarter of a billion dollars (c.$250 million) per annum via social media-enabled cryptomining malware or cryptojacking attacks.[37]

> *The number of enterprises affected by cryptojacking has doubled from 2017 to 2018.*

Inevitably, cryptojacking malware has had a notable impact upon social media platforms and their users. Up to 1 out of every 500 of the most searched-for websites have been estimated to now carry cryptojacking software[38] with social media representing 4 out of the top 5 websites and 11 out of the top 20.[39]

Applications, adverts and links have been the primary delivery mechanisms, but the use of Facebook Messenger has been especially instrumental in helping new strains, like Digmine, spread. Cryptojacking malware was also discovered on YouTube in 2018, where it was consuming more than 80% of a victims' CPU time to 'mine' Monero.[40]

Much of the cryptojacking malware originates from the Coinhive open-source mining code. It appears that social media users across Facebook, Instagram, Pinterest and LinkedIn have now all been exposed to links containing plug-ins based on this code.

[31] Godshall (2018)

[32] Alexandre (2018)

[33] Francis (2018)

[34] As a result of their failure to take down adverts hosted across their platform, legal actions have been advanced against Facebook, and Bitcoin adverts have since been banned on Facebook.

[35] CTA (2018), McAfee (2018)

[36] See methodology. Compare with similar findings in CTA (2018)

[37] See methodology.

[38] Musch et al (2017)

[39] DN Pedia (2018)

[40] BBC (2018)

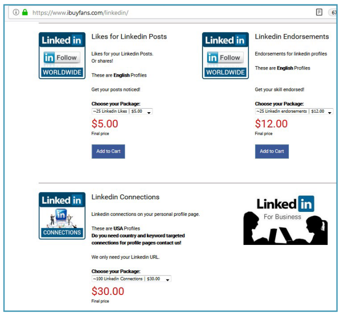
> *"Up to 25% of social media influencers may be involved in quasi-criminal manipulation, using fake followers and other misleading indicators of influence.*

For businesses, this type of malware can be very costly, with the increased performance draining IT resources and accelerating the deterioration of critical assets. Research suggests that the number of enterprises affected by cryptojacking has doubled from 2017 to 2018, with even large organisations such as Aviva and Tesla falling victim.[41]

Estimated revenues are not substantial for a single program (research suggests around $5 a day). But if amplification and contagion strategies work and enough of the cryptojacking software can be delivered through social media to victims' systems, a sizeable income can be generated.

BUYING TRUST THROUGH FAKE LIKES TO BOOST MALICIOUS PROFILES

If popularity and influence are a currency of persuasion across social media platforms, then it was only a matter of time before indicators could be converted to hard cash in the online economy. New kinds of criminal, or at least semi-legal opportunities, are now emerging as a result of key indicators of popularity on social media (such as the 'Like' function on Facebook, or 'Connections' on LinkedIn), and are being used to fuel revenues. This helps accounts to appear to be much more influential or credible than they actually are.



https://www.ibuyfans.com/linkedin/

Likes for Linkedin Posts

Likes for your Linkedin Posts.
Or shares!

These are **English** Profiles

Get your posts noticed!

Choose your Package:
~25 Linkedin Likes | $5.00

$5.00
Final price

Add to Cart

Linkedin Endorsements

Endorsements for linkedin profiles

These are **English** Profiles

Get your skill endorsed!

Choose your Package:
~25 Linkedin endorsements | $12.00

$12.00
Final price

Add to Cart

Linkedin Connections

Linkedin connections on your personal profile page.

These are **USA** Profiles
Do you need country and keyword targeted connections for profile pages contact us!

We only need your Linkedin URL.

Choose your Package:
~100 Linkedin Connections | $30.00

$30.00
Final price

Examples include:

- Up to 25% of influencers may now be involved in quasi-criminal manipulation, using fake followers and other misleading indicators of influence. In the case of one UK fashion influencer (who was paid £1,000 per post), it was found that 96% of her activity was fictitious and was mediated by bots.[42]
- Similarly, analysis of a single day's posts, where hashtags like #sponsored or #ad were used, found more than 50% fake engagements, with bots likely to be behind around 40% of comments on sponsored posts.[43]
- Leading brands like Ritz-Carlton may have had up to 72% of individuals reached by way of influencer strategies which turned out to be fake.[44]

> *"Social media 'Likes' can be purchased across a wide range of Dark websites – often at a higher value than credit card numbers.*

There is an emerging trade in 'Likes', which is being conducted both covertly and in plain sight. Research conducted for this project found that 'Likes' can be purchased across a wide range of Dark websites – often at a higher value than credit card numbers. Prices ranged from between $10-$20 for Facebook Likes, and from $5 for 25 likes on LinkedIn. Perhaps more useful for cybercriminals is the ability to purchase fake LinkedIn Connections, with prices starting from $30 for 100 connections. There are easily accessible, quasi-legal sites online like "Getsomelikes" or "Ibuyfans.com" that offer various packages of Likes, Followers or Connections. These often come from real accounts to add authenticity. Such sites offer discounts against competitors, customer service and support, business advice and tracking facilities.

As such, anyone, including cybercriminals, can easily buy influence to help them appear more credible and trusted, rendering the distribution of malware and manipulating employees and users into scams much easier.

[40] Redlock (2018)
[41] Greer (2016)
[42] Faull (2018)
[43] Faull (2018)

5.1 CRIMEWARE AS A SERVICE, IN PLAIN SIGHT

A striking finding of the research, which confirms the blur between legitimate and illegitimate platforms in driving the cybercrime economy, is the volume of crimeware or 'Cybercrime as a Service' tools and skills that are now available on social media platforms. In some cases, tools were found being offered openly and brazenly. In others, the platform served as a kind of marketing 'entry point' for goods and services, pointing toward more extensive shopping facilities on the Dark Web.

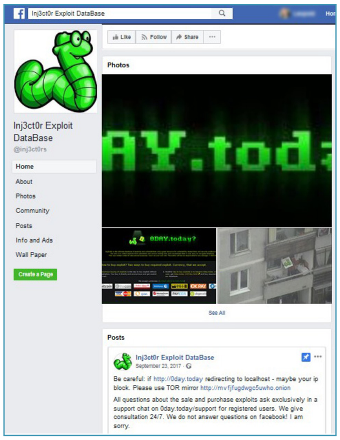
Given the sheer number of cybercrime tools now available, this research focused its searches, observations and attempted purchases on four key varieties of tools or commodities: *exploits, botnets, hacking services, and stolen data*. Of the searches that were conducted, up to 30% provided clear evidence that cyber tools could be easily obtained. This should be a real concern for organisations, because the ready availability of cybercrime tools will make it easier for hackers to obtain the instruments and services they need to launch an attack.

> *Ready availability of cybercrime tools makes it easier for hackers to obtain the instruments and services they need to launch an attack.*

EXPLOITS

The discovery of an exploit is not in itself illegal. Indeed, it can often be rewarded by software companies or related businesses who may be affected.[45] But if an exploit is sold on, knowing that it is going to be used to commit a crime, then there is a possibility of being charged as an accomplice. The legal ambiguities here have generated another grey economy in the trading of exploits, which borders legitimacy and criminality. Several sites on social media platforms were found to be openly vending exploits, including accounts such as:

- **The Injector exploit database** – an account offering the opportunity to trade in or to learn about exploits, which is readily accessible on Facebook. The site has over 96,000 followers and also advertises on Twitter
- **Exploit Packs** – this account, with over 4,000 followers, promises to contain a full set of 38,000+ exploits



Inj3ct0r Exploit DataBase
September 23, 2017

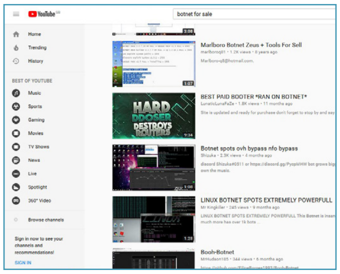
Be careful: if http://0day.today redirecting to localhost - maybe your ip block. Please use TOR mirror http://mvfjfugdwgc5uwho.onion

All questions about the sale and purchase exploits ask exclusively in a support chat on 0day.today/support for registered users. We give consultation 24/7. We do not answer questions on facebook! I am sorry.

Accounts like these often appear to convey a sense of legitimacy by offering their products for 'performing and conducting professional penetration tests'. However, given that there is no barrier to acquiring details of the exploits beyond login details, it is clear that such tools also offer a tempting 'how-to guide' to would-be hackers.

BOTNETS

Botnet hire appears to be readily available across most social media platforms. For example, on YouTube, one simple thematic search brought back over 200 results where botnets could be bought or hired.



botnet for sale

Marlboro Botnet Zeus + Tools For Sell
marlboroq81 • 1.2K views • 8 years ago
Marlboro-q8@hotmail.com.

BEST PAID BOOTER *RAN ON BOTNET*
LunaticLunaFaZe • 1.8K views • 11 months ago
Site is updated and ready for purchase don't forget to stop by and say

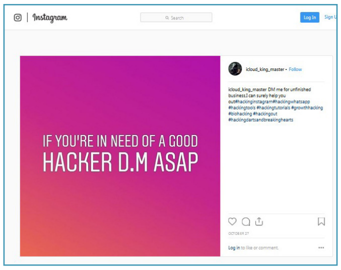
Botnet spots ovh bypass nfo bypass
Shizuka • 2.3K views • 4 months ago
discord Shizuka#0511 or https://discord.gg/PycpMHW bot grows big own the music.

LINUX BOTNET SPOTS EXTREMELY POWERFULL
Mr Kingkiller • 245 views • 9 months ago
LINUX BOTNET SPOTS EXTREMELY POWERFULL This Botnet is insan much more has over 1k bots ...

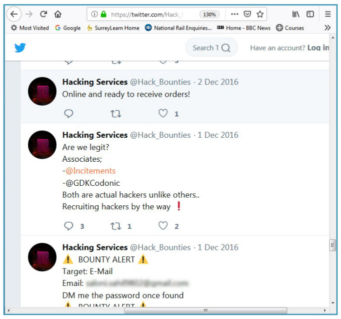
Booh-Botnet
MrHudson185 • 344 views • 6 months ago

Botnet and booter hires were also found on Facebook, Instagram, Twitter and other sites sampled for the research. Prices were fairly stable, with an average cost of around $10 a month for botnets with a full service package (including tutorials, technical support and other add-ons) or $25 for a no frills lifetime rental. The methods of advertising the services varied according to the format of each platform.

[45] Businesses pay researchers and white hats who discover vulnerabilities, with the size of the pay-out dependent upon how complex or dangerous the software flaw might be. We have therefore excluded such exploit hunting to focus on areas where there is malicious intent.


Instagram
Search
Log In
Sign U
IF YOU'RE IN NEED OF A GOOD
HACKER D.M ASAP
icloud_king_master • Follow
OCTOBER 27
Log in to like or comment.

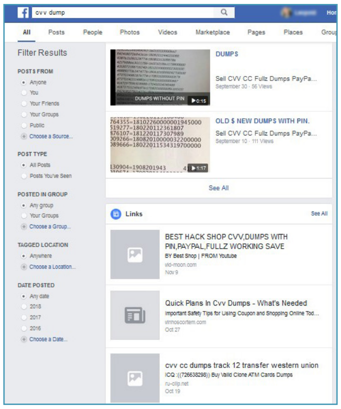
icloud_king_master DM me for unfinished business,I can surely help you out#hackinginstagram#hackingwhatsapp #hackingtools #hackingtutorials #growthhacking #biohacking #hackingout #hackingdartsandbreakinghearts



Hacking Services @Hack_Bounties · 2 Dec 2016
Online and ready to receive orders!
1

Hacking Services @Hack_Bounties · 1 Dec 2016
Are we legit?
Associates;
-@Incitements
-@GDKCodonic
Both are actual hackers unlike others..
Recruiting hackers by the way ❗
3 1 2

Hacking Services @Hack_Bounties · 1 Dec 2016
⚠️ BOUNTY ALERT ⚠️
Target: E-Mail
Email: [redacted]
DM me the password once found
⚠️ BOUNTY ALERT ⚠️



DUMPS
Sell CVV CC Fullz Dumps PayPa...
September 30 · 56 Views

OLD $ NEW DUMPS WITH PIN.
Sell CVV CC Fullz Dumps PayPa...
September 10 · 111 Views

BEST HACK SHOP CVV,DUMPS WITH PIN,PAYPAL,FULLZ WORKING SAVE
BY Best Shop | FROM Youtube
vid-moon.com
Nov 9

Quick Plans In Cvv Dumps - What's Needed
Important Safety Tips for Using Coupon and Shopping Online Tod...
vinhosocortem.com
Oct 27

cvv cc dumps track 12 transfer western union
ICQ :((726638298)) Buy Valid Clone ATM Cards Dumps
ru-clip.net
Oct 19

HACKING SERVICES

Around 30-40% of the social media sites inspected offered some form of hacking service. Very often there was an emphasis upon 'ethical' hacking services, though there were no obvious ways of corroborating this. Some examples uncovered during the research included: tools for hacking websites, hackers for hire, and hacking tutorials.

Other accounts involved more overtly criminal activity, such as credit card hacking services. However, repeat searches indicated that these appeared to close very quickly, either intentionally or because law enforcement or social media platforms intervened rapidly.
On Twitter, accessing the right kinds of accounts where hacking services could be obtained appeared to be a little more involved. However, with perseverance, a number of accounts where hacking services, legal or otherwise, could be obtained were found.

DATA TRADING AND SALE

Trading in stolen data for the use of account takeovers, financial gain, etc. involves more explicit criminality. Most prominent again were the 'grey economy' versions of this practice, where credit card numbers for sale were advertised, but with no suggestion that they had been stolen. It is fairly common to find services that enable purchasers to gain access to card details that are 'not stolen'. Instead, they can be used as proxies for enabling purchasers on sites where card details are required, without actually having to surrender their own details. Thus, many of the posts or adverts come with disclaimers such as:

> "**Disclaimer:** *The cards are to be used only for educational purposes. Do not use it to dupe or fraud people. It is an offence punishable by law and the user will be solely responsible."*

Some of the card data advertised are simply baits which, when clicked, start to download malware. The practice of advertising card dumps or CVV numbers on Facebook has been known for some time and such accounts are constantly being taken down by moderators, but numerous pages are still operating across Facebook and Twitter. There are also carding 'tutorials' offered on several platforms.

In contrast with Western social media sites, sales of card data or other personal information appear to be far more open and bold across Chinese social media. Recent research has indicated more than 30 user groups provide information on the QQ and Tieba Chinese sites, which are centred on selling and buying personal data. The price of such information ranges from 300 yuan ($43.64) per 100,000 data records up to 2,800 yuan for more authenticated varieties.[46]

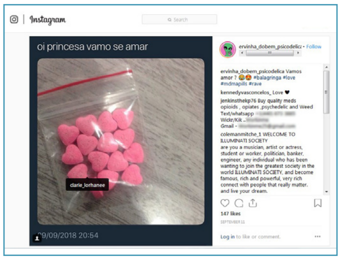
5.2 SOCIAL MEDIA'S ROLE IN TRADITIONAL CRIME

The illicit use of social media is not limited to cybercrime. It appears that a slew of more 'traditional' criminal activities are now taking advantage of the openness and reach of social media platforms. Perhaps the most obvious and well publicised examples of this involve the use of social media platforms for drug transactions and distribution. This research has also found a thriving criminal ecosystem involving other activities.

MILLENNIAL MONEY MULE RECRUITMENT – social media serves as a kind of recruitment centre, which brings together needy clients with a readily available labour force. Posts, feeds or adverts on social media highlighting opportunities to 'earn large amounts of money in a short time' are one part of this recruitment process, and there is no shortage of willing applicants.

[46] Reuters (2018)

Money laundering across social media has drawn in the kind of individuals not usually involved with crime – in particular, young millennials. Data obtained from CIFAS as part of this investigation suggests there could be as many as 8,500 money mule accounts in the UK owned by individuals under 21. Mule accounts for individuals as young as 14 were found. There appears to be an upward trend, with a 36% rise in the recruitment of money mules under the age of 21 since 2016 – most of this conducted via social media.[47] This suggests that teenagers may be the fastest growing demographic in the online money mule trade.



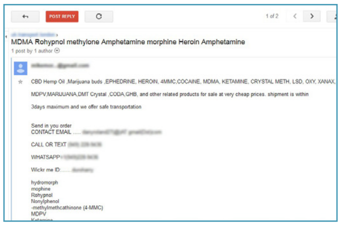
ervinha_dobem_psicodelica Vamos amor ? 😭😍 #balagringa #love #mdmapills #rave

kennedyvasconcelos_ Love ♥

jenkinsthekp76 Buy quality meds opioids , opiates ,psychedelic and Weed
Text/whatsapp [redacted]
Wickr/Kik .. [redacted]
Gmail - [redacted]

colemanmitche_1 WELCOME TO ILLUMINATI SOCIETY
are you a musician, artist or actress, student or worker, politician, banker, engineer, any individual who has been wanting to join the greatest society in the world ILLUMINATI SOCIETY, and become famous, rich and powerful, very rich connect with people that really matter. and live your dream.

147 likes
SEPTEMBER 11
Log in to like or comment.



[redacted] ›
MDMA Rohypnol methylone Amphetamine morphine Heroin Amphetamine
1 post by 1 author

[redacted]

CBD Hemp Oil ,Marijuana buds ,EPHEDRINE, HEROIN, 4MMC,COCAINE, MDMA, KETAMINE, CRYSTAL METH, LSD, OXY, XANAX, MDPV,MARIJUANA,DMT Crystal ,CODA,GHB, and other related products for sale at very cheap prices. shipment is within 3days maximum and we offer safe transportation

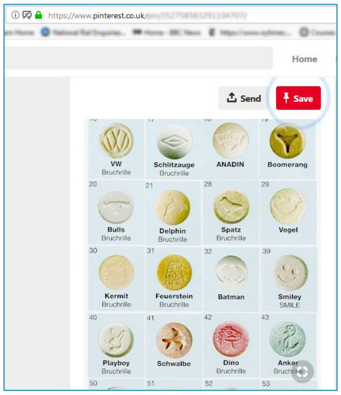
Send in you order
CONTACT EMAIL ..... [redacted]

CALL OR TEXT [redacted]

WHATSAPP [redacted]

Wickr me ID:....... [redacted]

hydromorph
mophine
Rohypnol
Nonylphenol
-methylmethcathinone (4-MMC)
MDPV
Ketamine



DRUGS – the usual perception of the online drugs market is of a shadowy, undercover affair conducted through Dark websites or specialised markets like the Silk Road. But the reach provided by social media platforms means that this is no longer the case.

Social media platforms are offering new avenues to support illegal online pharmacies offering prescription drugs. For example, research[48] suggests that up to 17% of pharmaceutical-related content on Facebook contains advertisements for illegal online pharmacies. A quarter of all posts about specific pharmaceuticals on Twitter and YouTube are presented as personal testimonials.

Research for this project also found a surprising availability of illegal drugs for purchase across such platforms, often sold openly and brazenly. Profits to individual suppliers could average up to $50,000 a month.[49] Platforms where such substances could be obtained include:

- **Twitter** – MDMA, amphetamines, cocaine and other drugs
- **Instagram** – MDMA, cannabis and opiates
- **Facebook** – Cannabis, GHB, cocaine for sale on private chats and groups
- **Google (Groups)** – Heroin, GHB, MDMA and Ketamine
- **Pinterest** – Ecstasy

FRAUD – It has been estimated that up to 20% of top brands' social media accounts are 'fraudulent',[50] with these accounts often used by criminals for further cybercrimes, including malware distribution or creation of phishing emails based on user information and preferences. Company executives are particular targets for fraud, with a worryingly high visibility on social media platforms where fraud is most prevalent, such as Facebook. Recent research suggests that, of those executives with a discernible online presence, 61% have a Facebook footprint compared to 31% with a LinkedIn footprint.[51]

Around 0.2% of social media posts examined by this report appeared to involve financial fraud of some kind.[52] Extrapolated more widely, this would indicate that fraudulent activities of various types generate upwards of **$290m** across social media per year. This suggests that criminal revenues from fraud enabled by social media have increased by more than **60%** since 2017, with research from 2017 estimating revenues (at the higher end) at around $180m.[53]

> *"Criminal revenues from fraud enabled by social media have increased by more than 60% since 2017.*

[46] Reuters (2018)
[47] Keyworth (2018)
[48] Tyrawski & DeAndrea (2015)
[49] Other research (BBC 2017) found comparable figures, with some suppliers boasting that within two days they could make profits of $30,000
[50] Gwynn (2016)
[51] CIFAS (2018)
[52] Details of this calculation can be found in the methodology section
[53] Zerofox (2017)

> *"Personal details and photographs are often stolen from Facebook sites to make dating scams more plausible.*

Online dating scams are another kind of fraud that has proved to be extremely lucrative, with reported losses for victims of more than $230m in the US alone[54] – though less than 15% of such crimes may ever be reported. In addition to such frauds being enacted on smaller, niche or specialist dating platforms, criminals have begun to target mainstream social media far more often. One woman in Texas lost nearly $2m, after criminals used information about her faith, which she had placed on Facebook, to befriend and then create a fake romance with her.[55] Details and photographs are also often stolen from Facebook sites to make dating scams more plausible.

VIOLENT AND HATE CRIME – whilst the online world appears to be one step removed from the realities of everyday violence, the ubiquity of social media means that it plays an enabling role. One example is how youth gangs use social media for recruitment or to incite rival gangs into violence. Mocking videos posted on YouTube, Snapchat and the like have been associated with increased aggression and fighting, sometimes with fatalities.[56]

A majority of former burglars (78%) suggested that social media platforms like Facebook have been used to target potential properties for burglary.[57] In one case, three men in New Hampshire confessed to using Facebook to burgle more than 18 houses.[58]

[54] Brenoff (2017)

[55] Brenoff (2017)

[56] Marsh (2018)

[57] Phillips (2016)

[58] Irshad and Soomro (2018)

6.1 RECOMMENDATIONS

> *Organisations must develop robust cybersecurity policies towards social media that include layered cybersecurity defences.*

SOCIAL MEDIA PLATFORMS

- Social media companies must take a much more active stance against the activities of cybercriminals exploiting their platforms. More must be done to clamp down on this activity to protect users and their data. This includes steps like making the hijacking of verified Twitter 'blue tick' account more difficult for cybercriminals.
- More must also be done to ensure social media platforms are not profiting from the acts of cybercrime. Infected adverts are all paid-for, and thus mean that the likes of Facebook, Twitter, Instagram and Snapchat could be profiting from the exploitation of their users. Instead, social media platforms should aim to ensure they either stop these revenues or donate these funds to a charity dedicated to fighting cybercrime and fraud.
- To reduce the influence of profiles, social media platforms need to do more to clamp down on fake followers, Likes and retweets that create the aura of authority, which will often result in users clicking on links.

ENTERPRISE

- Business needs to develop a much better understanding of how social media is used within the organisation and treat it as a back door into the enterprise that can be easily exploited. This not only includes being clear about which platforms benefit the organisation most effectively, but those that pose the greatest risks.
- Protection must extend beyond simply banning employees from social media platforms – ways around these restrictions can and will be found, creating a black hole for security teams.
- Organisations must develop robust cybersecurity policies towards social media that include layered cybersecurity defences, as well as encouraging better password hygiene (such as two-factor authentication) and controls over passwords that are reused across multiple platforms.
- Any protection must also consider the varying tactics between social media platforms – one fix cannot cover for everything. As such, organisations should consider the development of enhanced methods for the prevention of social engineering.

LAW ENFORCEMENT

- Policing and justice agencies should begin to redirect standard measures against cybercrime towards platform criminality, in particular activities that are being enacted through social media.
- The use of social media as an intelligence gathering tool needs to be supplemented with a greater awareness of its criminal risks.
- Enhanced training in detecting the varieties and types of crime that can be enacted through social media needs to be provided to officers.

CONCLUSION

GREGORY WEBB,
CEO of Bromium

This report shows that social media is a serious business risk to any organisation, leaving them wide open to attack. Current approaches to security simply do not provide the protection needed to prevent social media-enabled attacks from gaining a foothold in the enterprise.

It's vital that organisations understand and defend against this growing threat. The knee-jerk reaction to simply block social media websites is untenable. Organisations that fail to engage on social channels, whether it's LinkedIn, Twitter, YouTube, Facebook or Instagram will lose competitive advantage and fail to engage with a digital-native customer base.

So, what can businesses do?

> *"Application isolation provides a unique defence against social media-enabled crime.*

Organisations must ensure they fully understand the role played by social media in facilitating cybercrime, or risk being caught out by savvy cybercriminals intent on hijacking the enterprise. To do this, they must focus on reducing the business impact of social media-enabled crime by adopting layered cybersecurity defences and application isolation.

Application isolation provides a unique defence against social media-enabled crime by isolating web pages and attachments within hardware-enforced virtual machines. If a user clicks on a malicious link, or advert that contains malware, it is trapped and isolated from other applications and the network. This renders any malware harmless, leaving hackers with nowhere to go and nothing to steal. Once done, users can simply close their browser, deleting the virtual machine and any malware contained inside. This allows employees to get on with their job without worrying about causing a breach, dramatically reducing harm to organisations and safeguarding high value assets.

ABOUT BROMIUM

Bromium protects your brand, data and people using virtualization-based security via application isolation. We convert an enterprise's largest liability – endpoints – into its best defence. By combining our patented hardware-enforced containerization to deliver application isolation and control, with a distributed Sensor Network to protect across all major threat vectors and attack types, we stop malware in its tracks. Unlike traditional security technologies, Bromium automatically isolates threats and adapts to new attacks using behavioural analysis and instantly shares threat intelligence to eliminate the impact of malware. Bromium offers defence-grade security and counts a rapidly growing set of Fortune 500 companies and government agencies as customers.

Contact Bromium for more information about how application isolation and control can help you protect your employees on social media and how we can supplement your existing layered cybersecurity defences.

Visit our website: Bromium.com

Speak to a solutions expert: https://learn.bromium.com/contact-us.html

APPENDIX I

METHODOLOGY

Research for this project utilised a mixed methods approach, which combined quantitative analysis of data drawn from 10 social media platforms with the largest number of subscribers, with qualitative data drawn from interviews with social media users and observation of posts, comments and uploads, such as photos. This original data was supplemented with secondary data drawn from a comprehensive survey of key academic, business, law enforcement and other relevant data sources between 2015-2018.

The 10 major social media platforms that served as the sample for this research were:

- Facebook
- Instagram
- Twitter
- Snapchat
- YouTube
- Reddit
- LinkedIn
- Pinterest
- Tumblr
- WhatsApp

In addition, a selection of posts from the Russian and Chinese social media sites, including VKontakte and Odnoklassniki (Russia) and WeChat, QQ and Qzone (China), where translations or translators were available.

Across these platforms, a selection of more than 500,000 separate datapoints including posts, adverts or uploads, such as photos, were examined to search for activities such as malware distribution, crimeware sales and advertising, fraud, drug sales and other varieties of cyber-enabled crime. Where possible, covert observation and communication was established with social media users engaged in such activities to corroborate findings.

Note on calculation of criminal revenues enabled by social media:

ILLEGAL ONLINE PHARMACEUTICAL SALES

- Overall worth c.$400bn annually
- We know that around 17% of Facebook posts are related to illegal online pharma sales[59]
- 17% of $400bn = $68bn. But clearly not all of these 17% posts will actually generate any income
- To get a more accurate sense of possible revenues, we can use the average conversion rate for ecommerce websites (i.e. the calculated rate for turning ‘leads’ into customers) = 2.86%[60]
- 2.86% of $68bn = **$1.9bn** annually

FINANCIAL FRAUDS

- 0.2% of the 500,000 items examined appeared to relate to financial fraud or attempts to enact it
- Extrapolate to social media users – Facebook suggests it has 4.7bn new content items uploaded every day[61]
- Using 4bn as the baseline here – 0.2% of 4bn = 8,000,000 posts/ads etc. involving fraud

[59] Tyrawski & DeAndrea (2015)
[60] Saleh (2018)
[61] Zephoria (2018)

- Using the (very low) figure of just $1 of revenue per fraud, we can assume that $8m would be generated every day, $2.9bn over the year
- We know from reliable financial sources that around 2 out of every 3 frauds are prevented.[62] This implies that around 30% of attempted frauds may be successful. To further reduce uncertainty and to take into account other preventative factors, consider in turn that only 1 in 3 of these actually succeed in generating revenue. That is, a more conservative estimate of only around 10% of attempted frauds succeed in generating revenue
- 10% of $2.9bn = **$290m** annually

DATING FRAUDS

- Losses to victims in the US – $230m[63]
- Around 60% of individuals say they are using or have used social media in the form of dating platforms or apps[64]
- 60% of $230m = **$138m** annually

REVENUES FROM STOLEN DATA

- 4.5bn records were compromised in the 1st half of 2018 = 8bn rounded up for the whole year
- 56% of this was from social media (4.4bn)[65]
- The average value of stolen data is from $5 for credit card data; 'Fullz info' (billing address, PIN number, date of birth, social security number and even the maiden names of users and their online bank account credentials) – $20-$30[66]
- Bank account data – bank credentials that come with social security numbers, date of birth, billing addresses, maiden names and email addresses account for about 10% of value in account – say $200 for a $2,000 account
- Use the smallest level of recorded revenues – $5
- Assume not all data stolen via social media platforms is sold. Use similar conversion rate for ecommerce websites – 2.86%
- 2.86% of 4.4bn = 125,840,000 (*$5) = $629,200,000 (rounded up to **$630m**)

REVENUES FROM CRYPTOMINING

- There are around 500 million computers running cryptomining software[67]
- Of the 4bn users of the internet, we know that around 75% - around 3bn – have a social media presence[68]
- Given these two baseline stats, it can be assumed that around 375 million social media users may have been infected with some kind of cryptojacking software (75% of 500m)
- There have been differing estimates of the revenues generated by cryptojacking, but most agree that individual earnings are not very high at present. However low individual earnings are still consistent with cumulative revenues which are fairly high. Indeed, the fact that the numbers above look substantial may in itself be revealing, implying that though individual cybercriminals are not earning large amounts (and are probably using this as only one among their portfolio of activities), there are a lot of individuals who are trying this out (perhaps as part of the switch from revenues generated via ransomware attacks)

[62] UK Finance (2018)

[63] Brenoff (2017)

[64] Statista (2017)

[65] Gemalto (2018)

[66] DarkWeb News (2017)

[67] Olson (2018) https://www.csoonline.com/article/3262987/cyber-attacks-espionage/cryptomining-the-new-lottery-for-cybercriminals.html

[68] Global Digital (2018) https://wearesocial.com/uk/blog/2018/01/global-digital-report-2018

- For example, recent research suggests that browser-based mining is very low. It argues: 'On average, crytojacking websites attract 24,721 visitors per day and keep them for roughly 3 minutes. Overall, we thus observe a range of 0.17 to 89,000 core hours, with a mean of 1,550 core hours. With a hash rate of 80 H/s and Coinhive's payout ratio, a miner earns about $5.80 per day on average, which supports our observation that web-based cryptojacking currently provides only a limited profit'[69]
- Note, however, that above calculations relate to browser-based cryptojacking. The headline statistic above relates to revenues generated from crytptomining software illicitly installed on computers as a result of social media activity
- One estimate has suggested that a PC dedicated to mining could raise only between **$40 - $70** pcm[70] (with costs for electricity factored in)
- Again, though this is not that high individually, overall it would amount to cumulative revenues of around **$15bn** pcm – around **$180bn** per annum. (That is, using the lower-end revenue estimate of $40: 375m infected computers x $40 = $15bn pcm)
- This, however, seems implausibly high. So, consider an alternative baseline revenue estimate
- Another, more conservative, piece of research suggests that a 5,000 site attack might make just $24[71]
- Using the 375m SM user infected by such software, this figure would suggest revenues of **$1.8m** (375m/5000 = 75000; 75000 x $24 = $1.8m)
- This estimate would be based on just **one** attack. In principle, there could be multiple attacks conducted in the course of a single day. Conservatively, 1 attack per day translates to c.30 attacks per month, which results in revenues of **$54** pcm or **$648m** per annum
- This revenue – though more realistic-looking - derives from site-based crypto-attacks, rather than software illicitly installed on a PC
- To get a more accurate fix on this we can use recent data identifying the number of unique users attacked by mining malware. One plausible estimate suggests between 800,000 – 1m unique users were attacked in 2018[72]
- Using above statistic, assume 75% of these have a social media presence, which translates into 750,000 attacked by mining malware
- Assume less than 50% of these attacks succeed in downloading mining software = 375,000 unique users generating cryptomining revenues for cybercriminals
- Use lowest profit estimate ($40) detailed above. 350,000 x $40 = **$14m** revenues pcm or $168m per annum
- As a result, a plausible revenue range might be between **$168 - $648m** per annum. To be still more conservative, fix this at no more than **$250m**

Note that other forms of criminal revenue generation via social media, such as the sale of malware and hacking services, illegal drugs sales, etc. have not been included in this calculation since available data does not yet permit us to make any kind of reliable estimate. The level of criminal revenues is therefore likely to be much higher than this estimate.

[69] Musch et al (2018) https://arxiv.org/pdf/1808.09474.pdf

[70] Van Allen (2018) https://medium.com/finance-republic/heres-how-much-i-make-mining-crypto-with-my-gaming-pc-c692e46d38f# &

https://medium.com/finance-republic/heres-how-i-turned-my-crypto-mining-fail-into-a-wildly-profitable-machine-128f533aa62f

[71] Hern (2018) https://www.theguardian.com/technology/2018/feb/14/cryptojacking-campaign-24-dollars-hackers-cryptocurrency-salon

[72] Huillet (2018) https://cointelegraph.com/news/kaspersky-cryptojacking-increasingly-popular-attack-vector-for-botnets

APPENDIX II

A SELECTION OF SOCIAL MEDIA DATA BREACHES

YEAR	PLATFORM	LOSSES	METHOD
2018	**Facebook**	50m user records	A hack where attackers stole security keys which permit users to stay logged into Facebook
2018	**Reddit**	Volume not disclosed – username and hashed passwords, email addresses, and content, including private messages	Use of SMS intercept
2018	**Google +**	52m user records	Glitch in its platform which allowed external app developers to access the data
2017	**WeChat**	662m records of users exposed	Records probably accessed by Chinese Govt
2017	**VKontakte**	10m records including usernames, passwords, and email addresses	Use of old logins/ passwords
2016	**Myspace**	427m user records	Data discovered for sale from an earlier hack
2016	**LinkedIn**	117m	Method unclear
2016	**Twitter**	33m	Credentials obtained via infected browsers
2014	**Snapchat**	100,000	Method unclear
2013	**Snapchat**	4.9m phone numbers	Utilised the 'Find Friends' feature, which requires users to enter their phone number to see if other contacts are also using Snapchat
TOTAL OF USER RECORDS EXPOSED VIA SOCIAL MEDIA SINCE 2013 – CONSERVATIVE ESTIMATE		1.3 BN	

APPENDIX III

NICHE OR LOCAL SOCIAL MEDIA PLATFORMS AND CRIME

Three types of niche platforms were examined for this research. Examples and some of the risks users have encountered are listed below:

PARENTING PLATFORMS	MUMSNET, JUSTMOMMIES, FAMSTER, BABYCENTER, AND OTHERS
Mumsnet	Phishing emails and popups
	DDoS and swatting attacks (some facilitated via Twitter)
BabyCenter	Redirects from forum pages to malware. Malware and spam spread via mobile platform
Justmommies	Malware redirects
DATING PLATFORMS	TINDER, MATCH.COM, ETC.
Ashley Maddison	60 gigabytes of data hacked by the 'Impact team' hacking groups in 2016
Plenty of Fish	Browsers were redirecting users to exploits that installed malware in 2015
Fling.com	In 2017, 40m records compromised, including personal details, sexual preferences, orientation, and fantasies. Data from the site was being sold on the Dark web for around $400 (in Bitcoin)
FITNESS & MEDICAL PLATFORMS	PATIENTSLIKEME, FITMETRIX ETC
PatientsLikeMe	600,000 members who share data about their conditions, had data scraped by 3rd parties in 2017
MyFitnessPal	150m users had usernames, email addresses, and passwords (albeit encrypted) accessed in 2017
Singapore Medical Platform	1.5m records compromised, including those of the Singaporean Prime Minister

BIBLIOGRAPHY

Alexandre, A. (2018) New Study Says 80 Percent of ICOs Conducted in 2017 Were Scams, Coin Telegraph, 13/07/2018

Barker, S. (2018) Social media phishing on the rise as attackers experiment with tactics, Security Brief, 05/03/2018

Bean, S. 2017 UK workers waste over two hours a day on social media and other distractions, Insight, 24/8/2017

BBC (2016) How innocent photos of children have been exploited on Twitter, 28/11/2016

BBC (2017) Teens found selling drugs on Snapchat and Instagram, 14/07/2017

BBC (2018) YouTube caught out by coin-mining adverts, 29/01/2018

Boodai, M. (2011) LinkedIn Spam Emails Download Malware, Security Intelligence, 02/06/2011

Brenoff, A. (2017) How A Billion-Dollar Internet Scam Is Breaking Hearts And Bank Accounts, HuffPost, 20/07/2017

CIFAS (2018) Wolves on the Internet

Cimpanu, C (2018) One in Five Companies Gets Malware Infections via Social Media, Softpedia News, 05/04/2016

Cisco (2015) Midyear Security Report

Colleto et al (2016) Pornography Consumption in Social Media. Proceedings of the 10th International AAAI Conference on Web and Social Media. ICWSM 2016, May17-20, Cologne, Germany

Correa, D (2016) It's a trap! WhatsApp Gold 'premium' version lures users to malware, SC Media, 25/05/2016

CTA (2018), The Illicit Cryptocurrency Mining Threat, Cyber Threat Alliance, see: https://www.cyberthreatalliance.org/wp-content/uploads/2018/09/CTA-Illicit-CryptoMining-Whitepaper.pdf

DarkWeb News (2017) The Value of Stolen Data on the Dark Web, see: https://darkwebnews.com/dark-web/value-of-stolen-data-dark-web/

DN Pedia (2018) Top Million Websites & TLDs, see: https://dnpedia.com/tlds/topm.php

Faull, J. (2018) Influencer marketing fraud – how big a problem is it? The Drum 25/6/2018

FBI (2015-2017) Internet Crime Report

Francis, J. (2018) Researchers Find Over 15K Twitter Bots Pushing Cryptocurrency Scams, Bitcoin News, 13/08/18

Fraudwatch International (2018) Saving Face on Social Media, see: https://fraudwatchinternational.com/social-media/saving-face-social-media/

Frenkel, S., Isaac, M. & Conger, K. (2018) On Instagram, 11,696 Examples of How Hate Thrives on Social Media, New York Times, 29/10/2018

Gemalto (2018) Data Breaches Compromised 3.3 Billion Records in First Half of 2018, Press Release, 23/10/2018

Godshall, J. (2018), British Cyber Crime Center Reports $2.5 Million Lost in Cryptocurrency Scams This Summer, Unhashed, 11/08/2018

Greer, S. (2018) Social Chain wage war on fake Instagram influencers, Manchester Evening News 9/10/2018

Griffin, A. (2015) 10 million Twitter accounts could be deleted in porn purge to satisfy advertisers, Independent, 19/05/2015

Halevi, T., Lewis, J. & Memon, N. (2013) Phishing, Personality Traits and Facebook, see: https://arxiv.org/pdf/1301.7643v2.pdf

BIBLIOGRAPHY
CONTINUED

Hayes, N. (2016) Why Social Media Sites Are The New Cyber Weapons Of Choice, Dark Reading, 06/09/2016

Jay, J. (2018) Hackers still exploiting the human factor to carry out ransomware attacks, SC Media, 31/03/2018

Greer, S. (2018) Social Chain wage war on fake Instagram influencers, Manchester Evening News, 09/10/2016

Gwynn (2016) Fifth of top brands' social media accounts are 'fraudulent', Campaign, 01/09/2016

Irshad and Soomro (2018) Identity Theft and Social Media, IJCSNS International Journal of Computer Science and Network Security, 18, 1

Kaspersky (2018) Fake Facebook sites account for 60% of social network phishing in early 2018, 23/05/2018

Keyworth, M. (2018) I was a teenage 'money mule', BBC, 26/05/2018

Krustev, V. (2018) Facebook Nike Shoes Scam of 2018 Shows History Repeats Itself, Security Boulevard, 14/08/2018

KVRR (2017) Three Teams, 500+ Pills, One Snapchat Deception, see: https://www.kvrr.com/2017/03/31/three-teams-500-pills-one-snapchat-deception-leads-to-six-arrests-in-joint-nd-mn-drug-bust/

Leyden, J. (2017) Instagram phishing apps pulled from Google Play, The Register, 09/03/2017

Lo, C. (2018a) Almost 250 people in Hong Kong lose HK$1.9 million in WhatsApp scam, South China Morning Post, 11/04/2018

Lo, C. (2018b) Phone scammers now using WeChat voice messages to snare victims, South China Morning Post, 18/01/2018

McAfee (2018) June 2018 Threats Report

Marsh, S. (2018) Social media related to violence by young people, say experts, The Guardian 02/04/2018

Matthews, L. (2017) Russian Hackers Hid Link To Malware Servers In Britney Spears Instagram Comments, Forbes, 07/06/2017

Muller, K. & Schwarz C. (2018) Fanning the Flames of Hate: Social Media and Hate Crime, Warwick Business School, 19/02/2018

Mumsnet (2014) see: https://www.mumsnet.com/Talk/site_stuff/1957616-What-is-with-the-random-redirect-to-porn

Musch, M. et al (2017) Web-based Cryptojacking in the Wild, Technische Universität Braunschweig Institute for Application Security

Palmer D. (2018) This password-stealing malware uses Facebook Messenger to spread further, ZDNet, 01/05/2018

Pesce et al (2012) Privacy attacks in social media using photo tagging networks: A case study with Facebook, PSOSM'12 April 17 2012, Lyon, France

Pew (2016) "Social Media and the Workplace", Pew Research Center, June, 2016

Pew (2017) News Use Across Social Media Platforms 2017, Pew Research Center, September, 2017

Phillips, G. (2016) The Dark Side of Social Media, Mud, 31/10/2016

Powell, J. (2018) The Problem With Banning Pornography on Tumblr, New York Times, 06/12/2018

Ragan, S. (2015) Malware uses video and tags to infect 100,000 people on Facebook, CSO, 30/01/2015

Redlock (2018) Lessons from the Cryptojacking Attack at Tesla, 20/02/18

BIBLIOGRAPHY
CONTINUED

Reynolds, J. (2018) Mentions of social media in crime quadruple in four years, Shropshire Star, 22/01/2018

Reuters VoA 2018 China Sees Surge in Personal Information Up for Sale, 23/08/2018

Saleh, K. (2018) The Average Website Conversion Rate by Industry (updated November 2018), Invesp, see: https://www.invespcro.com/blog/the-average-website-conversion-rate-by-industry/

SANS (2017) Threat landscape survey: Users on the front line, White paper, 2017

Seymour, J. & Tully, P. (2016) Weaponizing data science for social engineering: Automated E2E spear phishing on Twitter, Black Hat Conference

Statista (2017) Share of internet users in the United States who have used online dating sites or apps as of April 2017, by age group, see: https://www.statista.com/statistics/706499/us-adults-online-dating-site-app-by-age/

Tambini, Damian (2018) Social Media Power and Election Legitimacy. In: Tambini, Damian and Moore, Martin, (eds.) Digital dominance: the power of Google, Amazon, Facebook, and Apple. Oxford University Press, New York, NY, pp. 265-293

Thomas (2013) Trafficking Fraudulent Accounts: The Role of the Underground Market in Twitter Spam and Abuse, Usenix Security Symposium

Tsing, W. (2018) Maybe you shouldn't use LinkedIn, Malwarebytes, 05/04/2018

Tyrawski, J. & DeAndrea, D. (2015) Pharmaceutical Companies and Their Drugs on Social Media: A Content Analysis of Drug Information on Popular Social Media Sites, J Med Internet Res. 2015 Jun; 17(6): e130

UK Finance (2018) Banks and card companies prevented £2 in every £3 of attempted unauthorised fraud in 2017, see: https://www.ukfinance.org.uk/finance-industry-stops-1-4-billion-in-attempted-fraud/

Vishwanath, A. (2015) Habitual Facebook Use and its Impact on Getting Deceived on Social Media, Journal of Computer-Mediated Communication, 20, 83–98

WMC (2012) Pinterest users finding unwanted porn pinned, 20/9/2012, see: http://www.wmcactionnews5.com/story/19590096/pinterest-users-finding-unwanted-porn-pinned/

Zephoria (2018) The Top 20 Valuable Facebook Statistics, see: https://zephoria.com/top-15-valuable-facebook-statistics/

Zerofox (2017) External social and Digital threats to Financial institutions, whitepaper

Bromium®

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.