CC-DRIVER

Researching cybercriminality to design new methods to
prevent, investigate and mitigate cybercriminal behaviour.

R1 — Landscape Study of Cybercrime-as-a-Service

WP2 — Scoping Cybercriminality and Technical Capabilities

Abstract

In this report, we present a landscape study of Cybercrime-as-a-Service. We focus on the range of activities, the providers, the prices, and their business model. Activities of Cybercrime-as-a-Service include: (i) Cryptocurrency laundering and tumbling, (ii) Bulletproof hosting, (iii) Tutorials, training and consulting, (iv) Hacking-as-a-Service, (v) Coding/Programming-as-a-Service, (vi) Crypting - obfuscation, (vi) Distributed denial-of-service (DDoS) attacks/Reflection attacks (DRDoS), (vii) SMS flooding and spamming, (viii) Escrow/Garant/Treuhand, (ix) Email spamming and phishing, (x) Crimeware - Ransomware-as-a-Service, (xi) Serial keys - pirated software, (xii) Social boosters - friends and “likes” for purchase, (xiii) Web traffic - visitors, (xiv) Cybercriminal business, marketing and messaging.

Key words: Cybercrime, technical drivers, human drivers

Contributors

Lead

FORTH – Evangelos P. Markatos

Other

- University of East London
- Valencia Local Police
- SIMAVI
- Polícia Judiciária
- F-Secure
- BayHfoeD

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 883543.

Contents

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 883543.

Executive summary

Over the past years, we have seen cybercrime evolving from a set of narrowly-scoped and disconnected activities to a full-fledged business model. Indeed, as cybercrime evolved, cybercriminals became more skilled in and more focused on specific aspects of their work: some were good at programming, some were good at managing, some were good at trading credit cards, and some were good at recruiting money mules. It seems that everyone was good at something - but almost nobody was good at everything at the same time. As a result, cybercriminals needed each other to cooperate. Thus, they created teams, markets, inputs, outputs, and they started to collaborate with each other trading their services and pulling their skills together.

At the same time, cybercriminals realised that their competence, despite how narrow it was, was still in high demand: people needed a fake identity, they needed access to another account, or they just needed a way to get even with their competitors. And where there is a need, there is a way: Cybercrime-as-a-service came just in time to fill this need.

As a result, Cybercrime-as-a-Service, benefiting from economies of scale, has significantly lowered the bar for new cybercriminals to engage in all forms of cybercrime that were not possible before. Today we see a wide variety of criminal activities being offered in a "Cybercrime-as-a-Service" model including but not limited to: (i) Cryptocurrency laundering and tumbling, (ii) Bulletproof hosting, (iii) Tutorials, training and consulting, (iv) Hacking-as-a-Service, (v)

Coding/Programming-as-a-Service, (vi) Crypting - obfuscation, (vi) Distributed denial-of-service (DDoS) attacks/Reflection attacks (DRDoS), (vii) SMS flooding and spamming, (viii) Escrow/Garant/Treuhand, (ix) Email spamming and phishing, (x) Crimeware - Ransomware-as-a-Service, (xi) Serial keys - pirated software, (xii) Social boosters - friends and "likes" for purchase, (xiii) Web traffic - visitors, and (xiv) Cybercriminal business, marketing and messaging.

In this report, we analyse all the above mentioned modes of Cybercrime-as-a-Service and explain how cybercrime evolves over time and space.

List of figures

List of tables

List of acronyms/abbreviations

Abbreviation	Explanation
2FA	Two-factor Authentication
ACSC	Australian Cyber Security Centre
AML	Anti-Money Laundering
APA	American Psychiatric Association
APT	Advanced Persistent Threat
BBS	Bulletin Board System

BEC Attacks	Business Email Compromise
BTC	Bitcoin
CaaS	Cybercrime-as-a-Service
C&C	Command-and-Control
ccTLD	Country Code Top-level Domain
CERN	European Council for Nuclear Research
CERT-In	Computer Emergency Response Team-India
CGI	Computer-generated Imagery
CIS	Commonwealth of Independent States
CMA	Computer Misuse Act
COE	Council of Europe
CPE	Common Platform Enumeration
CPS	Cyber-physical System
CSAM	Child Sexual Abuse Material
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
CVV	Card Verification Value
CWE	Common Weaknesses Enumeration
DaaS	Data-as-a-Service
DDoS Attacks	Distributed Denial of Service Attacks
DGA	Domain Generation Algorithm
DNS	Domain Name System
DOJ	U.S. Department of Justice
DoS Attacks	Denial of Service Attacks
DRDoS Attacks	Distributed Reflection Denial of Service Attacks
DRT	Detection & Response Team
ENISA	European Union Agency for Cybersecurity
EoP	Elevation of Privilege
FBI	Federal Bureau of Investigation
FDA	Food and Drug Administration
FTP	File Transfer Protocol
FUD	Fully Undetectable
GPL	General Public License
GPS	Global Positioning System
GST	General Strain Theory
HPP	Hackers Profiling Project
HRaaS	Hacker Recruiting as-a-Service
HTaaS	Hacker Training as-a-Service
HTTP	Hypertext Transfer Protocol
IAM	Identity and Access Management
ICS	Industrial Control Systems
IP	Internet Protocol

IRC	Internet Relay Chat
ISO	Optical Disk Image
ISP	Internet Service Provider
IT	Information Technology
IaaS	Infrastructure-as-a-Service
IoT	Internet of Things
JRE	Java Runtime Environment
JRR	John the Ripper
KYC	Know Your Customer
LEA(s)	Law Enforcement Agency (Agencies)
LoL	League of Legends game
MBR	Master Boot Record
MSP	Managed Service Provider
MaaS	Malware-as-a-Service
MIT	Massachusetts Institute of Technology
NCA	British National Crime Agency
NCCU	UK's National Cyber Crime Unit
NIST	National Institute of Standards and Technology
NKC	National Cybercrime Cooperation Centre
NSE	NMAP's Scripting Engine
NTP	Network Time Protocol
NVD	National Vulnerability Database
OSI	Open Systems Interconnection
OSVDB	Open Source Vulnerability Database
OWASP	Open Web Application Security Project
P2P	Peer-to-peer
PII	Personally Identifiable Information
PoE	Path of Exile game
PUA	Potentially Unwanted Application
PyPI	Python Package Index
PoC	Proof of Concept
QRF	Quick Reaction Force
RaaS	Ransomware-as-a-Service
RAT	Remote Access Trojans
RBN	Russian Business Network
RCE	Remote Code Execution
RDP	Remote Desktop Protocol
SCADA	Supervisory Control and Data Acquisition
SEO	Search Engine Optimization
SIM	Subscriber Identity Module
SMB	Server Message Block
SMS	Short Message Service

TCP	Transmission Control Protocol
TDS	Traffic Directing Server
TTL	Time to Live
UDP	User Datagram Protocol
URL	Uniform Resource Locator
VGCA	Vietnam Government Certification Authority
VNC	Virtual Network Computing
VPN	Virtual Private Network
VPS	Virtual Private Server
VR	Virtual Reality
WVD	WhiteSource Vulnerability Database
XSS	Cross-Site Scripting
ZAC	Zentrale Ansprechstelle Cybercrime

Table 1: List of acronyms/abbreviations

Glossary of terms

Term	Explanation
Ransomware	Malicious software that encrypts the files of a user and asks for money (ransom) in order to decrypt them

Table 2: Glossary of terms

1 Cybercrime-as-a-Service (CaaS)

In recent years, cybercrime has adopted practices similar to those of legitimate businesses.[1,2] For example, full cybercrime solutions are offered ***as-a-service*** and ***on-demand*** to interested customers (such as aspiring cybercriminals) (Hyslip, 2020). This model is called ***Cybercrime-as-a-Service*** (CaaS) and has become an increasingly popular trend in the area of cybercrime.

> “ CYBERCRIME HAS MATURED INTO A LARGE PROFIT-DRIVEN INDUSTRY.
>
> *Jonathan Lusthaus – author of "Industry of Anonymity"*

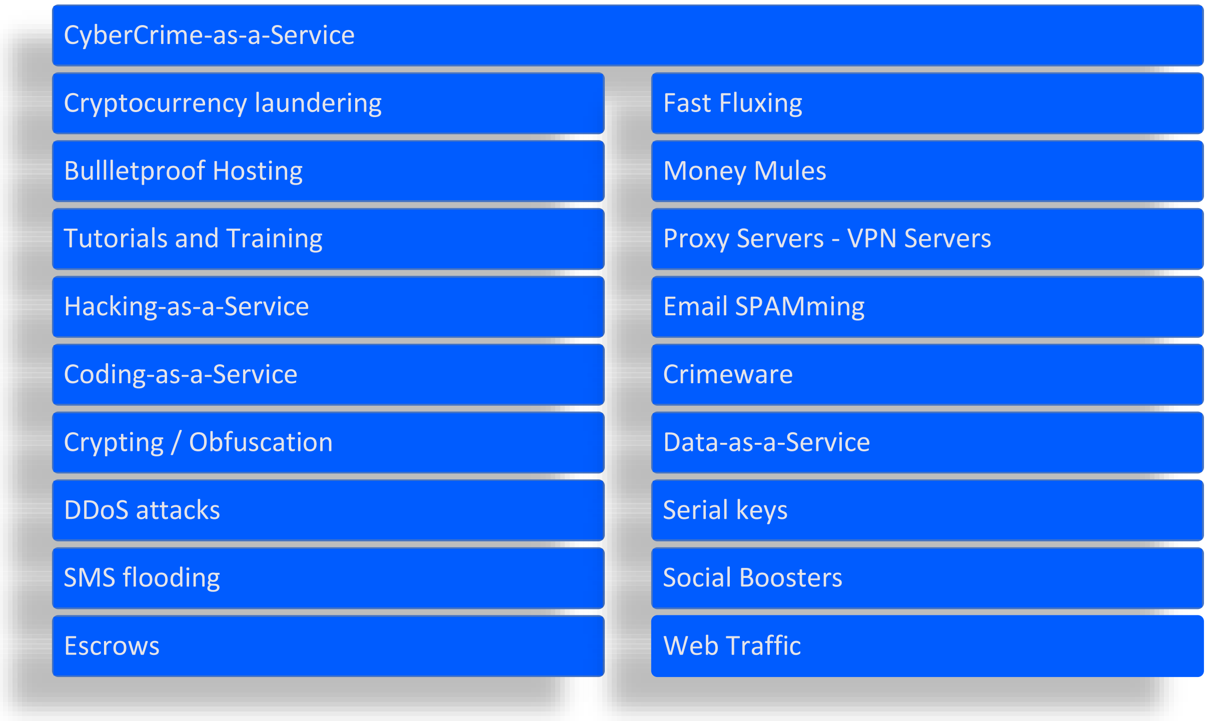
CaaS has led to the industrialisation of cybercrime. On the one hand, cybercriminals with technical knowledge monetise their skills by offering their services and products for sale in a simple and easy way (i.e. "as-a-service"). On the other hand, individuals with little or no technical knowledge are now able to purchase these services, as well as any other required digital assets, and thus easily join the world of cybercrime (Europol, 2014; Wainwright & Cilluffo, 2017). CaaS has become an umbrella term for services and illegal products that are involved in many known cybercrimes, including (i) distributed denial-of-service (DDoS) attacks, (ii) phishing attacks, (iii) ransomware, (iv) malware distribution, (v) email spamming, (vi) bulletproof hosting, etc. All the different phases of a cybercrime, such as (i) malware development and testing, (ii) infection, (iii) distribution and spreading, (iv) monetisation and laundering, etc., are performed by cybercriminals who are experts in the particular area and then become available for sale to new cybercrime participants or other cybercriminals, thus enabling affiliate cybercrime groups that cooperate (Wainwright & Cilluffo, 2017). Research has shown that selling products and services is less risky, and could be more profitable for hackers than committing the crime itself (Manky, 2013). That is, cybercriminals can make money by selling malware instead of using this malware to compromise computers themselves!

Consequently, CaaS can be considered as a generic and modern technical driver for cybercrime, as a new generation of aspiring criminals can now commit illegal cyber operations, when otherwise they would not have been able to do so (Manky, 2013). In this section we list (cybercrime-related) products and services that are available for sale and, in this way, facilitate cybercrime operations. Although both buyers and sellers of the following, not exhaustive list of services are involved in cybercrime, they have different technological skills and expertise. In most cases, buyers are technologically inexperienced while sellers are technical experts (Trend Micro, 2016a).

[1] https://www.welivesecurity.com/2016/12/08/cybercrime-business-model-value-chain/

[2] https://www.iotworldtoday.com/2017/06/14/8-strategies-transition-product-service-business-model/

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.



CyberCrime-as-a-Service

Cryptocurrency laundering

Bullletproof Hosting

Tutorials and Training

Hacking-as-a-Service

Coding-as-a-Service

Crypting / Obfuscation

DDoS attacks

SMS flooding

Escrows

Fast Fluxing

Money Mules

Proxy Servers - VPN Servers

Email SPAMming

Crimeware

Data-as-a-Service

Serial keys

Social Boosters

Web Traffic

Figure 1: Offerings for "Cybercrime-as-a-Service". Aspiring cybercriminals may purchase these offerings on-line and thus ease their way into conducting cybercriminal activities.

1.1 Cryptocurrency laundering and tumbling

Cryptocurrencies are widely used to extort or launder money coming from illicit cybercrime operations, or from traditional crimes such as kidnapping and terrorism. Cryptocurrencies allow anonymity (or at least pseudonymity) which makes it difficult for law enforcement agencies (LEAs) (to trace the cybercriminals themselves. The vast majority of cybercriminals use cryptocurrencies for their operations and are very careful to avoid linking their cryptocurrency accounts with their real identity. However, this identification is necessary in the process of converting cryptocurrency money into real-world money through banks or exchanges. To this end, services have been created that allow criminals to launder their cryptocurrencies and withdraw them without being caught. This instance of CaaS is called cryptocurrency **laundering** and occurs through the process of "**tumbling**" or "**mixing**".

> *To hide illegal transactions, cybercriminals mix their money transfers (i.e. "tumbling" them) with legitimate money transfers into one composite transaction with several senders and several receivers at the same time!*

Tumbling is the process of mixing identifiable cryptocurrency funds with others in order to obfuscate their provenance, possession and movement. To illustrate it with a simplified example, suppose that cybercriminal A would like to send one coin to cybercriminal B. Suppose also that legitimate user C would like to send one coin to legitimate user D. The tumbler would take both requests and create a new "transaction". This transaction has two inputs: one coin from A and one coin from C and two outputs: one coin goes to B and one coin goes to D. However, it is not clear which of the two outputs got the cybercriminal's coin. Was it B or D? Without knowing this information, LEAs find it very difficult to trace the cybercrime money.[3] Although in this simple example, there seem to be only two choices, both of which LEAs may choose to trace, the repeated application of mixing increases the number of choices to the point where it is practically impossible to trace all of them. Originally, tumblers were created to improve the anonymity of the Bitcoin cryptocurrency, which uses a public ledger for transactions, but they soon became another instance of CaaS, used for illegally obtained funds. Tumblers mix together "clean" and "dirty" crypto coins by executing a series of random exchanges between them, thus generating and returning a set of randomised coins. Apart from the mixing server, none of the parties can identify the origin of the outgoing coins. Typically, tumblers take 1-3% as a transaction fee for their operations.

In December 2013, a hacker stole more than US $100 million in bitcoins from a site for drug dealers called Sheep Marketplace and tried to hide the money by using various tumblers.[4] In February 2015, a tumbler called Bitcoin Fog was used to launder more than 7000 BTC that were stolen from Bter, a China-based Bitcoin exchange.[5] The founder of the Bitcoin Fog tumbler was arrested in April 2021 on charges of money laundering of over 1.2 million bitcoin at a value of approximately $335 million at the time of the transactions.[6] During 2017, about $266 million was laundered through cryptocurrencies and, in the next year, this amount tripled ($761 million) in the first half of 2018.[7]

Cybercriminals also use unregulated cryptocurrency exchanges that hide customer information in order to launder money. One such example is the WEX/BTC-e cryptocurrency exchange, which was allegedly responsible for cashing out 95% of all ransomware payments made from 2014 to 2017 (Lewis, 2018).[8] In 2020, just in the Bitcoin ecosystem, $3.5 billion were sent from criminal addresses (controlled by dark markets, ransomware actors, hackers, etc.). These bitcoins will eventually end up in a cryptocurrency exchange from which they will be laundered and converted to ordinary currency.[9]

In 2018, Bitconnect was forced to shut down by regulators because it was suspected of being a Ponzi scheme. As a result, the cryptocurrency crashed from almost $500 to less than a dollar.[10] A

[3] One might say that LEAs will trace both B and D. But this soon becomes exponential if B and D join another tumbler, and then another, and another.

[4] https://www.businessinsider.com.au/a-thief-is-attempting-to-hide-100-million-in-stolen-bitcoins-and-you-can-watch-it-live-right-now-2013-12

[5] https://thenextweb.com/news/chinese-bitcoin-exchange-bter-will-pay-back-users-after-losing-1-75-million-in-cyberattack

[6] https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer

[7] https://www.americanbanker.com/news/crypto-money-laundering-rose-3x-in-first-half-2018-report

[8] https://cointelegraph.com/news/pwc-bitcoin-ransomware-hackers-laundered-money-via-wex-exchange

[9] https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/

[10] https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-scam-bitconnect-cryptocurrency-regal-coin-a8945291.html

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

Bitconnect token was among the top 20 cryptocurrencies in the world in terms of market value in early 2018.[11] Subsequently, the former head of BitConnect was arrested in India for promoting another cryptocurrency called "Regal coin", promising high returns (up to 45% per month); this also turned out to be a scam.[12]

However, countermeasures have been put in place over time to make this kind of activity more difficult and to regulate cryptocurrency exchanges.

KYC (Know Your Customer) is a process used in exchanges to verify the customer's identity so as to eliminate the illegal use of cryptocurrency and to decrease tax fraud.[13] This process has been mainly used by banks (and similar financial services), so that banks get to know the real identity of their customers in order to reduce financial fraud and money laundering. Although most exchanges have enabled KYC, some less-known exchanges still allow their customers to buy cryptocurrency without identity verification, thus facilitating the active involvement of cybercriminals in cryptocurrency trading. To evade the KYC policy even further, cybercriminals may transfer their money from one cryptocurrency to another. And finally, they may use tumblers and mixers so as to blur any traces that may lead to them (see above).

In addition to KYC, another process named AML (for Anti-Money Laundering) monitors customers' transactions to determine if they are legitimate or not.[14,15]

1.2 Bulletproof hosting

Cybercriminals, operating by definition in cyberspace, need a server to host their illegal activities. Bulletproof hosting provides this service.

Cybercriminals need a lot of infrastructure (such as web servers and web hosting) in order to operate their businesses successfully. Moreover, it is very important for them to maintain these infrastructures at peak performance and availability during operations. However, legitimate ISPs and web hosting firms may detect, report, and block illegal actions performed through their servers and networks, causing cybercriminals to continuously seek hosting services that are "bulletproof": that is, hosting services that are not easily "taken down". Such hosting services allow their customers to host content (such as malware) and perform operations (such as spamming) that would be considered illegal and would not be allowed by other hosting services. Even further, such bulletproof hosting services are usually hosted in faraway countries. This implies that any legal action will involve several legal jurisdictions before any court order is issued, so that if and when a legal process is completed it will have taken a long time. Even when legal action is taken, and when a court order is issued, such hosting services usually delay the execution of any court order as long as possible, buying even more time for their customers. As a result, through a combination of legal loopholes, complicated legal processes and

[11] https://www.fool.com/investing/2017/07/20/the-20-largest-cryptocurrencies-by-market-cap.aspx
[12] https://quickpenguin.net/regalcoin-scam/
[13] https://paybis.com/blog/what-is-kyc/
[14] https://shuftipro.com/blog/anti-money-laundering-compliance-for-crypto-exchanges-2021-update/
[15] https://www.forbes.com/sites/vishalmarria/2018/09/13/eu-5th-anti-money-laundering-directive-what-does-it-mean/

unwillingness to cooperate, such hosting services allow their customers to perform their activities for quite some time.

Bulletproof hosting is an instance of Infrastructure-as-a-Service (IaaS) (Europol, 2014) that can be found in many underground markets. Typically, these providers operate in countries from Asia and Eastern Europe, which have more relaxed laws and regulations about cybercrime and illegal Internet activity. Domain and web hosting firms that operate in these countries also allow their customers considerable leniency in the kinds of material they may host and distribute.[16]

Regarding the content, in most cases, criminals use bulletproof services to distribute and host (i) fake shopping sites, (ii) torrent sites, (iii) phishing sites, (iv) malware, (v) command and control components, (vi) e-mail spamming components, and (vii) illegal material such as child abuse images (Goncharov, 2015c).

Prices of bulletproof services that were recently found on the Dark Web can range from $200 to $250 US per month depending on the illegal service that will be hosted on the server (Hyslip, 2020). Other offerings, found in the underground markets of North America, are sold at cheaper prices and provide a standard server with 100GBs of storage, 2GBs of memory and one IP address for $75 US per month (Wilhoit & Hilt, 2015). In the underground markets of Brazil, buyers can find bulletproof hosting services that start from $15 US per month and can reach the price of $2000 US per month for services with protection from DDoS attacks and other extra features (Trend Micro, 2015a). In the equivalent markets of China, services that include protection from DDoS attacks cost from $81 to $775 US per month (Gu, 2013). Today, prices found in clearnet websites seem to be the same or even lower compared to the past. For example, a bulletproof VPS hosting could cost $19-137 US per month and a premium plan for bulletproof web hosting could cost about $58 US per month.[17]

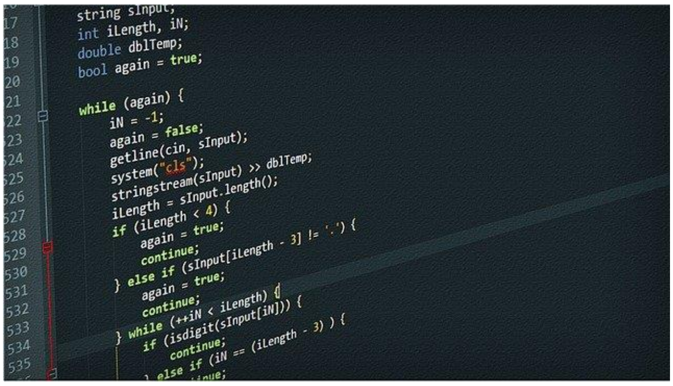
Although bulletproof hosting is usually robust, there are cases where it has been taken down. Some notable examples of bulletproof service providers that have been taken down are those of the Russian Business Network (RBN) in November 2007, the US-based McColo in November 2008, 3FN in 2009, MaxiDed in 2018 and CyberBunker in September 2019.

1.3 Tutorials, training and consulting

Individuals with technical knowledge in various aspects of cybercrime may offer advice and consulting services in underground forums. These products and services are important to users who enrol in such underground forums and seek to find hacking knowledge, tactics, and tips on malware tools. These forums may sell guides, links, tutorials on cybercrime operations and hacking tools, providing an excellent venue for aspiring cyber criminals to gain knowledge from their tutors.

[16] https://us.norton.com/internetsecurity-emerging-threats-what-is-bulletproof-hosting.html
[17] https://www.websiteplanet.com/web-hosting/bulletproof-hosting/

Such resources can advance the capabilities of an individual to commit cybercrime and are considered as a generic technical driver of cybercrime. Apparently, individuals with little to no hacking skills gain cybercrime knowledge by simply consuming tutorials or by buying consulting services from cybercrime practitioners. In some cases, these goods are even offered free of charge. One reason is that cybercriminals aim to introduce as many newcomers as possible to cybercrime. In this way, the community of cybercriminals will grow and income from trading other CaaS offerings will be potentially increased.



```
string sInput;
int iLength, iN;
double dblTemp;
bool again = true;

while (again) {
    iN = -1;
    again = false;
    getline(cin, sInput);
    system("cls");
    stringstream(sInput) >> dblTemp;
    iLength = sInput.length();
    if (iLength < 4) {
        again = true;
        continue;
    } else if (sInput[iLength - 3] != '.') {
        again = true;
        continue;
    } while (++iN < iLength) {
        if (isdigit(sInput[iN])) {
            continue;
        } else if (iN == (iLength - 3) ) {
```

Since offering consulting and training services related to cybercrime is illegal, most of these services are sold online on the Dark Web. To further increase anonymity, payment is usually arranged through cryptocurrencies. Thus, most of the transactions remain anonymous by using Bitcoin or Litecoin. As an example of these CaaS offerings, cybercriminals in Brazil offer programming and training services by selling tutorial videos and providing support via Skype. Indeed, one provider of such a service advertises that customers could be trained to create remote access trojan (RAT) software for the price of $46 US. Another advertisement promises to teach customers to commit bank frauds for the price of $579 US (Mercês, 2014).

On the Dark Web, it is possible to find plenty of websites offering consulting, training and tutorials at different costs, depending on the provider. It is easy to find services such as hacking different types of online accounts (social media, email), hacking servers, spying on a computer or performing DDoS attacks. Tutorials are also sold explaining how to make a botnet, set up a remote access, or other topics related to phishing and credit card fraud.[18]

Prices depend on the complexity of the attack or training, but some offered services are very affordable and the price could be paid almost by anyone. In some cases, having technical knowledge is not even required.

1.4 Hacking-as-a-Service

Cybercriminals frequently provide “Hacking-as-a-Service”. That is, they receive requests to compromise (hack) user accounts. The most common requests include hacking (i) email accounts and (ii) accounts on social networking platforms (Europol, 2014). Methods used by cybercriminals to hack their way into user accounts include (i) brute forcing, (ii) social engineering, and (iii) leveraging vulnerabilities at websites (Goncharov, 2012).

Brute forcing is the process of automatically trying different passwords based on a dictionary file until the one that works is found. Brute forcing requires a considerable amount of time and it is not very likely to guess strong passwords. When brute forcing is not effective, cybercriminals bypass password authentication using answers to “secret questions”. Such questions include

[18] As this chapter is predominantly focused on category 1 cybercrimes, some cybercrimes, while they may have been mentioned, are not the focus of this chapter and fall outside of the chapter’s scope and aims, for example online child sexual abuse or exploitation.

"Where did you go to school?", "What is the name of your first pet?", etc. Secret questions are used by platforms to give users an option to reset their accounts when they lose access to it. Users usually provide easy-to-guess answers. Criminals take advantage of such opportunities and acquire access to an account by resetting the password.

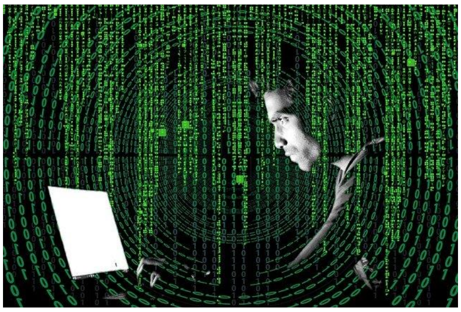
More experienced criminals manage to get access to accounts by using sophisticated techniques that exploit vulnerabilities that may exist in the websites. Such attacks include SQL injections and Cross-Site Scripting (XSS). Popular platforms such as Gmail, Facebook, Twitter and Instagram use enhanced security measures to protect their users against hacking. In such cases it is a common practice for criminals to use social engineering techniques along with malware (trojans and sniffers) in order to capture passwords and get access to the victims' accounts. The cost for hacking a Facebook or a Gmail account is $100-120 US, with no guarantee of success (Goncharov, 2015a). Similar[19] or slightly higher prices[20] can be found on either clearnet or Dark Web sites for hacking social accounts (in Instagram, WhatsApp, Telegram, Twitter, etc.), complete websites, databases, smart phones and so on.[21] At this point, we should also add that in some of the cases such advertisements are just scams that steal the money from clients.

1.5 Coding/Programming-as-a-Service

When someone needs a programmer to build a malicious application they could look for an offer in the CaaS ecosystem where such advertisements are posted. Effectively, this "Programming-as-a-Service" places programming in the service of cybercriminals.

Examples of such offers can be found in Russian underground markets. Prices are formed based on negotiations between the customer and the programmer and depend on the complexity of the software to be developed, the required timeline and the reputation of the programmer. As an example, a programming service advertisement requested about $1300 US for a Trojan for bank account stealing (Goncharov, 2012).

1.6 Crypting - obfuscation



Crypters are programs that are used to obfuscate (i.e. change the form of) malware in order to bypass the detection techniques of antivirus systems. Antivirus systems may be based on static analysis (i.e. they have an idea of what the *structure* of malware looks like) and pattern matching (i.e. they know that the malware contains specific strings). To avoid detection via static analysis and pattern matching, crypters change the malware to make its

[19] https://socialhacking.pro/

[20] https://www.instabitnetwork.com/pricing/

[21] https://hireahacker.ninja/

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

detection by antivirus systems very difficult, if not impossible. To achieve their goal, crypters may use a variety of methods, including:

- **Encrypt** the body of the malware. If the antivirus system scans the (now encrypted) malware it will not be able to recognise any meaningful structure. Obviously, when the malware is executed, it has to be decrypted. If each instance of the malware is encrypted with a different key, antivirus systems will not be able to find any common patterns between two different instances of the same malware. Typically, the final output of a crypter is the encrypted malware payload packaged with a crypter stub (i.e. the decryptor), which contains the decryption key. The stub is a standalone program or just a piece of code used for the decryption, loading, and execution of the final malicious payload.
- **Change** the body of the malware by adding instructions that seem to perform a lot of operations, but do not have any effect on the computation that the malware does. One may think of such crypters as "adding" an extra program to the malware, a program that seems to do a lot of work, but which in fact does not change the essential malicious operation of the malware. This "extra" program may be interleaved with the malware code, appended at various places, and do an enormous amount of computation, as long as the functionality of the malware remains intact.

Crypters that prevent all security programs from detecting a specific malware are called FUD crypters which stands for "fully undetectable" while others that only work in some cases are called "partial" crypters and are cheaper in the market (Mercês, 2014).

A variation of crypters can be found in the market under the name **joiners** or **binders**. These programs are designed to join two or more files together into a single file. As an example, the joiner can create an image file which is an apparently innocent file until the user opens the image and executes the bound malware.

Crypting is another popular CaaS offering in underground markets. Offerings include (i) the sale of the actual crypter, and (ii) the provision of the service of a crypter. In the first case a simple crypter could cost only $17 US or even less (Trend Micro, 2015a; Mercês, 2014). As in most cases, the more complicated the service, the greater the price will be. For example, a crypter with a polymorphic engine can be sold for more than $100 US (Goncharov, 2015a).

In the latter case, crypting service providers first check the malware of their customers against most anti-malware tools available in the market to see if it gets detected. Then, they encrypt the payload and repack the product into a new one that is undetectable. Services out there cost from $20 US for a one-time single file crypt to $1000 US per month for crypting an unlimited number of files (Wilhoit & Hilt, 2015). Other advertisements, found within an English-language underground forum that was also accessible via a clearnet website, offered access to the crypting service for $49 US per month, while in Russian-language underground forums the average price of similar services was predominantly under $100 US per month.[22] The popular RAZ crypter can be found for rent for $25 US for one month or $40 US for three months.[23]

[22] https://www.recordedfuture.com/user-friendly-loaders-crypters/

[23] https://www.recordedfuture.com/user-friendly-loaders-crypters/

1.7 Distributed denial-of-service (DDoS) attacks/Reflection attacks (DRDoS)

> “Would you like to disable the web servers of your competitor?
>
> —Rent a DDoS Attack Service!

Denial-of-service (DoS) and reflection attacks are very popular types of cyberattack. Cybercriminals use such attacks in order to take down (or disrupt the operations) of a victim website. To do so, attackers send an overwhelming amount of requests to the victim, essentially flooding its computing and communication capacity. Such attacks (or the threat of such attacks) can be used to request ransom, to settle disputes, or even to call attention to a political cause. DoS targets include big companies, financial institutions and governments.

To avoid being detected, DoS attackers usually use a false (fake) source IP address.[24] In this way they cannot be easily detected by the victim. To amplify their attack, attackers send their requests to the victim from a distributed set of computers. This is usually called a Distributed Denial of Service attack (DDoS). DDoS attacks are very difficult to stop, because even if some of the attack computers are stopped, the rest will continue their operation.

DDoS attacks were actually one of the first CaaS offerings, dating back to almost the beginning of this century. Prices depend on the length and the size of the attack. Buyers and providers typically communicate through forums and messaging apps (see section 3.3) and after payment is received, the provider executes the DDoS attack. Prices are fairly affordable. For example, some advertisements found in the Russian underground markets involve a full day DDoS service for $10-140 US (Goncharov, 2015b), while a one-week service costs $150 US and a one-month service costs $1200 US (Goncharov, 2012). In 2021, a DDoS attack of 10-50k requests per second to an unprotected website cost $50 US for one day, $500 US for one week and $1000 US for one month. In the case of a premium protected website, a DDoS attack of 20-50k requests per second cost $200 US for one day.[25] Another advertisement found on the Dark Web offers a DDoS attack (200k requests per second for three hours) at a price of about $60 US.[26]

Over the last years, subscription services called “**stressers**” have appeared on the market (Hyslip & Holt, 2019). These services essentially “stress” a target web server in order to see how robust it is, how much load it can sustain, and possibly find its breaking point. Although stressers sound like a good idea, they can easily be abused for DDoS attacks. Cybercriminals that subscribe to this type of service launch their own DDoS attacks through a web-based front end. This scenario enables non-technical criminals to easily conduct DDoS attacks and increase the number of such attacks globally. Prices for stressors are also affordable. For example, some advertisements found in North American underground markets promise 125 GBps for 5 minutes at the price of $25 US, or $60 US for about half an hour (Wilhoit & Hilt, 2015).

[24] This is equivalent to sending a torrent of physical mail to a victim using a fake sender address. In this way, the victim does not know who is responsible for this torrent.

[25] https://www.privacyaffairs.com/dark-web-price-index-2021/#9

[26] https://www.welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices/

A variation of the DDoS attack is the DRDoS "**reflective denial of service**" attack. In this type of attack, public servers, such as open DNS resolvers or NTP servers, are used to reflect the attack to the victim. The attack works as follows:

- The attacker sends a request to the reflector pretending to be the victim computer.
- The reflector services the request and provides the response to the victim—since the attacker pretended to be the victim.
- The attacker repeats the same process with several different reflectors.
- Ultimately, all these reflectors respond to the victim, overwhelming it with (unsolicited) responses to requests that the victim never made. If enough reflectors are used, the victim will eventually be swamped with traffic.

Obviously, one can say that the victim can ignore all these unsolicited requests. This is true. However, these requests consume the victim's download bandwidth, and possibly some of the victim's computing capacity. If the responses are too many, they will eventually deplete the resources (bandwidth and computing capacity) of the victim.

In March 2013, a massive attack targeted the Spamhaus Project, an organisation based in Geneva, Switzerland and London that maintains a database of domain names and IP addresses involved in spam-related and malicious activities. The attackers ultimately targeted Tier 1 providers, which operate the networks at the core of the Internet, and Internet Exchanges (IX), and generated more than 300 Gbps of attack traffic. The method of attack used in this case was DNS reflection.[27] The attack was traced back to a Dutch company named Cyberbunker, which wanted revenge on Spamhaus for putting the company in its spamming databases.

These attacks are difficult to block, because legitimate servers are used to generate the malicious traffic. It is also challenging to find the source of the attack.

Mitigating against DDoS or DRDoS can be difficult but there are many ways to do it. None of the methods work alone to prevent everything, so in order to properly defend against these kinds of attacks, several of them need to be implemented around the internet. These methods are, for example, ingress filtering (BCP 38), scrubbing the traffic, load balancing and blackholing.

BCP38, also known as ingress filtering, is for ISPs or others who deploy edge network hardware. BCP38 is used to defend against source address spoofing, which is used typically in DRDoS attacks. BCP38 is used at the edge of the network, where it inspects the incoming packets' source headers for their source IP. If this source address in the source headers do not match the allowed IP address range, it is dropped for source address spoofing.[28]

Scrubbing of the traffic is used to mitigate against typical DDoS attacks. When the service provider, for example an ISP, detects a DDoS attack, they may reroute the traffic to a separate location that is known as a scrubbing centre. These scrubbing centres have high network capacity, so they try to handle the flood of packets from the attack and identify the malicious traffic and discard it. Then the non-malicious traffic is routed back to the original destination. Since DDoS attacks can scale up to 1 Tbps and even higher, scrubbing centres are highly costly, as the hardware and bandwidth to

[27]https://www.networkworld.com/article/2164810/ddos-attack-against-spamhaus-was-reportedly-the-largest-in-history.html

[28] https://www.rfc-editor.org/rfc/rfc2827.txt

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

handle that kind of traffic flood is expensive. Also, identifying the malicious traffic can be difficult, as attackers can use different network protocols in their attacks.[29]

Some providers, the like Content Delivery Network service provider Cloudflare, are also providing DDoS mitigation by taking advantage of their huge network capacity. They use load balancing to distribute the traffic they receive to multiple servers in their data centres, so that basically all of their servers participate in the mitigation process if needed. One way to do this is with anycast routing.[381,30] This kind of mitigation for the largest attacks requires enormous network capacity, which only few organisations have.[31]

In blackholing, the traffic is rerouted to a null route or black hole and dropped. Blackholing, in its basic form, reroutes both malicious and legitimate traffic, and this can also have the same end result as the initial DDoS attack itself, where the requested service is not available.[32]

One newer type of an attack is referred to as bit-and-piece attack. The reason for this kind of an attack is the stealth it tries to achieve by using numerous different IP addresses from multiple IP prefixes and only sending a small amount of data to the target IP prefix from a single source. This is done to evade detection of the attack and make the mitigation much harder. These attacks tend to be smaller in size, so they would bypass the threshold for junk traffic, but can result in a denial of service when a large number of IP addresses take part in the attack.[33]

1.8 SMS flooding and spamming

SMS SPAM is an unsolicited message sent to a mobile phone for commercial or malicious purposes. SMS spamming services are available underground and promise to send SMS messages to mobile phones. Prices range from $155 US for 5000 text messages to $1159 US for 100,000 messages (Mercês, 2014). Additionally, tech-savvy customers can get an application with a support and lifetime licence to send an unlimited number of SMS spam messages by themselves for the price of $193 US. This scenario could cost less money, but there is also more risk for the customer to get traced. It also requires a 3G modem that can be purchased and shipped for $50 US (Mercês, 2014).

Similar to traditional DDoS attacks, SMS flooding attacks have also been offered as a service on underground marketplaces. This kind of attack targets individual phones by sending a very large number of SMS messages. This attack makes the cellular service for both messaging and phone calls unavailable to the user. Depending on the magnitude of the attack, a local cellular network can be affected and even be disabled across a region. An SMS flooder that could send 2 SMS per second would cost only $16 US (Goncharov, 2012).

[29] https://blog.cloudflare.com/no-scrubs-architecture-unmetered-mitigation/
[30] https://www.cloudflare.com/learning/cdn/glossary/anycast-network/
[31] https://blog.cloudflare.com/reflections-on-reflections/
[32] https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/
[33] https://blog.nexusguard.com/threat-report/ddos-threat-report-2019-q1

1.9 Escrow/Garant/Treuhand

> *Cybercriminals do not trust each other!*
> *They us a trusted-third-party (an Escrow) for their business.*

Although cybercriminals need to collaborate with each other, they do not necessarily trust each other. For example, when cybercriminal Alice wants to purchase something from cybercriminal Bob, how does she know that Bob will deliver what he promised if Alice pays in advance? On the other hand, if Alice does not pay until she receives the purchased products/services, how does Bob know that he will get paid at the end? To solve this dilemma, escrows were introduced. An escrow is a trusted third party who receives and sends money on behalf of the primary parties of a transaction. Since the beginning of the Internet, escrows have been around and have participated in auctions and online commerce transactions. This development was introduced to enhance trust and provide additional security and anonymity in online dealings. In this way, buyers and sellers reduce their chances of falling victim to a scam, and platform providers ensure that everyone gets what they were expecting.

Escrow systems are popular in cybercriminal forums and are officially offered to the members of the forum to ensure smooth transactions. Typically, a senior member of the forum has the role of the trusted escrow. Once a deal has been agreed, the buyer sends the funds to the escrow and then receives the goods from the seller. Once the buyer has confirmed that the product or the services meet the legitimate expectations and the deal's agreed conditions, then the escrow releases the funds to the seller. Escrows take a percentage cut of the funds as a payment for their services,[34] typically 1-15%[35] of the amount that will be paid (Trend Micro, 2015b). We can draw distinctions between the popularity of escrow services on different Dark Web forums, based on the language of the forum. For instance, escrow is most popular and used in Russian-speaking forums—to the extent that it is formalised with a built-in setup. The setup includes a designated forum guarantor, who acts as the neutral third party in the escrow transactions[36].

Contrast this to the English-speaking forums, where the use of an escrow is rather informal. There, the forums usually have assigned individual members who are flagged as possible third-party candidates to act as the neutral third party. These individual members take incoming requests on an ad-hoc basis. The use of an escrow on the English-speaking forums is not as popular as it is on the Russian-speaking forums.

Finally, we can analyse the way the situation is handled on German-speaking forums. The use of an escrow is commonplace there, where it is known as "Treuhand". The usual method of Treuhand follows closely on the methods of escrow. Some German-speaking forums, however, have taken a different approach and developed an escrow system known as "Multisig". Multisig operates with the principle of having both the buyer and seller first enter their cryptocurrency wallet keys. A multi-signature cryptocurrency wallet will be generated, into which the buyer can deposit their funds. Once the deal has been confirmed and package delivered, the money can be released from the generated wallet to the seller. The upside of this system is that at least two of the three participants have to agree upon the transaction, before any money is delivered in any direction.

[34] https://www.digitalshadows.com/blog-and-research/escrow-systems-on-cybercriminal-forums/
[35] https://www.deepwebsiteslinks.com/bitcoins-escrow-services/
[36] https://www.digitalshadows.com/blog-and-research/escrow-systems-on-cybercriminal-forums/

The use of Multisig ensures that the guarantor (third, neutral party) cannot take the funds for themselves, which is still technically possible in the more traditional escrow system. The additional layer of security brings further assurance into the entire ordeal for all participants.

1.10 Fast-Fluxing - a moving target

Cybercriminals frequently use the computers they compromise in order to perform their malicious activities. Indeed, they use those computers to host illegal services, to send SPAM, to send copyrighted content, etc. To avoid being blocked, cybercriminals use a large number of compromised computers in a round robin fashion: a small set of computers serves illegal material for a small amount of time, then another set of computers undertakes this task, then another set takes their place, then another, and so on and so forth. In this way, cybercriminals evade (or at least delay) detection. Indeed, by the time LEAs (or security practitioners) detect the IP address of a computer involved in malicious activities, another compromised computer will have taken its place. Effectively cybercriminals implement a “moving target” that makes it difficult for LEAs to detect.

To implement this “moving target” (or “fast fluxing”, as it is called), cybercriminals may make extensive use of the DNS translation on the Internet. DNS is the protocol (and the infrastructure) used to translate a domain name (e.g., www.google.com) into an IP address (e.g., 216.58.214.132). Each such translation comes along with a timeout (or TTL: Time to Live): this means that the translation (from domain name to IP address) is only valid for a time equal to TTL, a value that ranges from a few seconds to several minutes or longer. After the TTL expires, the translation is no longer valid: the client needs to ask the DNS server again.

Cybercriminals abuse TTLs in the DNS infrastructure as follows: First, they purchase a malicious domain name, say www.malicious.com. Then, they compromise a number of computers. And finally, they repeatedly “register” and “de-register” those computers as IP addresses for www.malicious.com. In this way, each translation request for www.malicious.com will return a different IP address. Effectively, the hosting of the domain name www.malicious.com hops quickly from one computer to another. In this way, the actual computer that serves a request for www.malicious.com changes frequently. When LEAs eventually find an IP address that corresponds to www.malicious.com, this information may be out of date, as this IP address will probably not serve www.malicious.com any longer.

This ever-changing set of pointing IP addresses makes it extremely difficult for authorities to create blacklists and finally block these IPs. Eventually, the list of IP addresses will become so large, and the information in it will become so out-of-date, that traditional firewalls and other signature-based prevention systems will not be able to cope with these types of adaptive threats. And this is exactly the goal of cybercriminals: to create a botnet infrastructure that cannot be stopped by blacklists and firewalls!

In 2007, the Storm Worm was one of the first pieces of malware that made use of this technique to change the IP addresses for its command & control servers. During the next few years, the Avalanche group, an international criminal syndicate involved in phishing attacks, online bank fraud and ransomware, implemented a double fast flux infrastructure on 800,000 domains

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 883543.

(Wainwright & Cilluffo, 2017).[37] DarkCloud is another Fast-Flux infrastructure that has been active since at least 2014. Most of the compromised hosts from this infrastructure were located in Ukraine, Russia and Romania. This network hosted ransomware, trojans, email spam, C&C components and more.[38] During 2018, researchers observed a new Fast-Flux infrastructure that used Fast-Flux domains that were previously assigned to known nodes of DarkCloud. This new network was named SandiFlux and its nodes were concentrated in Romania and Bulgaria.[39]

Fast-Fluxing services are offered as a CaaS from botnet herders in underground markets and hacking forums (Trend Micro, 2015b).

1.11 Mules

A money mule is the individual who makes profit by transferring (actually **laundering**) illegally acquired goods or funds on behalf of others. Mules receive money from a third party in their bank account and transfer it to another one or take it out in cash and give it to someone else, obtaining a commission for it. Mules are critical parts of the fraud supply chain and are a CaaS offering (Money Laundering-as-a-Service; Europol, 2014) in underground forums and the Dark Web.[40]

> “ DO YOU WANT YOUR ILLEGAL PROFITS TO APPEAR IN A LEGITIMATE ACCOUNT IN THE STATES?
>
> —HIRE A MONEY MULE!

However, in many cases, mules have been recruited by cybercriminals and are unaware that they are participating in illegal operations. Sometimes, criminals have also obtained PII and personal documents from the mules that can then be used in other CaaS operations. Typically, a mule is recruited through phony job scams (e.g., “money transfer agents”), spam emails, social networking sites or even on the streets by a scam operator. Mules are mostly young unemployed people or newcomers to a country seeking work (Europol, 2014). Their job will be to receive and transfer amounts of money to third parties through their bank accounts or just to take it out in cash and give it to someone else.[41] Mules are not involved in the crimes that generate the illegal funds, but they can be considered as accomplices to the crime and eventually may go to jail. In 2010, the FBI Cyber Crimes Task Force charged more than 37 defendants for their involvement in the laundering of the money of compromised bank accounts of the Zeus trojan.[42] Reportedly, these mules facilitated the transfer of more than US $3 million.

[37] “It takes a network to defeat a network”: in December 2016, Europol, the Public Prosecutor’s Office Verden and the Lüneburg Police (Germany), the United States (U.S.) Attorney’s Office for the Western District of Pennsylvania, the U.S. Department of Justice (DOJ), the U.S. Federal Bureau of Investigation (FBI), Eurojust and the Joint Cybercrime Action Taskforce (J-CAT) along with a network of international law enforcement and trusted partners successfully took down the Avalanche group.

[38] https://krebsonsecurity.com/2016/05/carding-sites-turn-to-the-dark-cloud/

[39] https://www.proofpoint.com/us/threat-insight/post/sandiflux-another-fast-flux-infrastructure-used-malware-distribution-emerges

[40] https://www.rsa.com/en-us/blog/2016-04/money-mules-the-critical-cash-out-service-in-the-fraud-supply-chain

[41] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling

[42] https://archives.fbi.gov/archives/newyork/press-releases/2010/nyfo093010.htm

Another category of mules is the "re-shipping" mules. In this scenario, the operators of the scam purchase goods with stolen money and send them to the mules. The mules reship the goods back to the operator or other fraudsters in order for them to make the goods available in the local black market. Most "re-shipping" mules are cut loose after one month of operation or before they receive their first payment, leaving them exposed to face prosecution and charges. Studies have shown that the revenue from the reshipping scam is estimated at US $1.8 billion per annum.[43]

As the FBI states in its "Common scams and crime"[44] report, individuals advertise their services as a money mule (probably on the Dark Web), to include what actions they offer and at what prices.[45] Moreover, mule advertisements have also been observed in Japanese underground bulletin board systems (BBSs), where cybercriminals exchange various messages and job opportunities (Urano, 2015).

1.12 Proxy servers

Proxy servers are appliances or applications that have the role of the intermediary in the resource requests and responses between a client and a server. For example, if Alice would like to request a web page from web server W, she requests the web page from a proxy P who, in turn, requests the web page from W and delivers it to Alice. In this way, Alice "hides" her identity from W. As far as W is concerned the request came from P, not from Alice. As long as P does not keep log files, investigations from LEAs are unlikely to reveal the fact that it was Alice who requested the web page from W in the first place.

> "
> **HIDE YOUR IP ADDRESS WITH A PROXY SERVER!**

Proxy servers can be used for various purposes, but the one that makes them popular among the network of cybercriminals is their ability to provide some form of anonymity: i.e., the web server W and its ISP do not know that the web page request came from Alice. Proxy servers are popular in underground markets and are available as a CaaS offering, usually next to advertisements of bulletproof hosting services (Goncharov, 2015a). Cybercriminals tend to be more trustful of the proxies found in underground markets, provided by fellow cybercriminals, rather than the ones that are provided by legitimate vendors. Indeed, although the web server W does not really know that it was Alice who requested the web page in the first place, the proxy P knows that it was Alice. Thus, Alice has to trust that P will not (or better yet cannot) provide this information to LEAs.

The types of proxy servers described below are the more frequent ones on the markets and could be organised into chains by the user in order to further improve the provided anonymity:

- HTTP/FTP proxies: process the HTTP protocol and operate between a web server and a web client, such as a web browser. Sometimes, these proxies also support the FTP protocol. All modern browsers support the use of HTTP proxies.
- SOCKS proxies: operate in the Layer 5 of the OSI model (the session layer) and forward TCP connections to an arbitrary IP address while providing means for supporting the UDP protocol (SOCKS 5). Despite the fact that SOCKS proxies are more wide-reaching compared

[43] http://www0.cs.ucl.ac.uk/staff/G.Stringhini/papers/shipping-ccs2015.pdf
[44] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules
[45] https://www.commercial-bank.com/userfiles/filemanager/61794706gop6pznpm7p2/

to the HTTP proxies, programs must have been explicitly developed to support the SOCKS protocol, otherwise additional software has to be installed for this reason.

- CGI proxies (anonymisers) provide a webpage with a form that accepts input from users.[46] The user visits the CGI proxy webpage via a common browser and enters in the form the URL that she wants to access. Then by submitting the request, the user gets onto the page via the CGI proxy. By using such proxy servers, users can anonymously surf the Internet without using additional software or changing the settings of their browsers.

Examples of offerings found in underground markets include the selling of lists of hundreds or even thousands of HTTP/SOCKS proxies for less than US$5 US, and dedicated proxy services at prices that vary per duration of use (e.g., 5 days/$4, 10 days/$8, 30 days/$20, 90 days/$55) (Goncharov, 2012).

1.13 VPN Servers

A virtual private network (VPN) extends a private network across a public network and enables users to operate as if they were directly connected to the private network. Most VPN services enable encrypted connections, thus providing a secure channel for communications. Much like proxies, VPN servers can be abused by cybercriminals to enhance their anonymity. Indeed, using a VPN, cybercriminals are able to hide their source IP as the traffic appears to be initiated from the network of the VPN service provider. VPN servers can also be used to provide access to content restricted by geographical regions. For example, a cybercriminal located in country A may not be able to access content in country B if this content is served only to computers (i.e., IP addresses) of country B. To overcome this limitation, the cybercriminals may use a VPN with a presence in country B, and in this way their IP address will appear to originate from country B.

However, as reputable VPN providers may keep a record of connections and other sensitive information, VPNs are not always the preferred choice for cybercriminals who seek complete anonymity. Therefore, other affiliate cybercriminals offer VPN services with enhanced trust and security properties that ensure complete anonymity. Such services are available for sale in underground marketplaces with an average price of about $100-200 per year, $5 per day or $10 per week (Goncharov, 2012; Goncharov, 2015a; Wilhoit & Hilt, 2015).

In December 2020, a coordinated operation led by Europol and LEAs took down a large VPN service used by criminals to carry out malicious activity. This VPN was used for over a decade to spy on and compromise companies with ransomware attacks.[47]

Another aspect of cybercrime related to VPN servers is the compromise of companies' networks. The COVID-19 pandemic has changed the way people work. Working remotely from home is now common, and many companies had to adapt their infrastructure to allow such new practices by installing VPN servers. In 2020, vulnerabilities have been disclosed for some proprietary software,

[46] See, for example, https://www.proxysite.com/ and https://hide.me/en/proxy.

[47]https://www.europol.europa.eu/newsroom/news/cybercriminals%E2%80%99-favourite-vpn-taken-down-in-global-action

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

such as Pulse Secure, Palo Alto GlobalProtect and Fortinet FortiGate VPN products. By exploiting these vulnerabilities, threat actors were able to access companies' network, harvest passwords and deploy ransomware.[48]

1.14 Email spamming and phishing

Spamming is the process of sending unsolicited bulk emails, which contain commercial advertisements and possibly all kinds of malicious links, to a large number of recipients. Email spamming is one of the most common methods attackers use to spread malware. Nowadays, the COVID-19 pandemic and the increased worldwide interest in the virus have contributed to the growth of spam emails across the globe. The virus opened up the floor for new junk email story lines and introduced a population of newly home-based workers who had no previous experience with spam. F-Secure's report (F-Secure, 2020) entitled "Attack Landscape H1 2020", presents a deluge of COVID-19 themed emails containing a mixture of spam, phishing attempts, and malicious attachments, as cybercriminals capitalised on the fear and uncertainty generated by the COVID-19 crisis. Specifically, in 2020, about 51% of attempted malware infections arrived by email, compared to 43% in 2019.

Many countries were targeted by spam campaigns as soon as they announced their first COVID-19 infections. Emails that supposedly contained information on preventing the spread of the virus had malicious attachments. One of the first of these targeted Japan in January 2020. The email content informed recipients about the rapid spread of the virus and instructed them to download a Word document attachment with further preventive measures. Victims had to click on the "Enable Content" button to be able to view the document, thus enabling the Emotet payload (see 5.1.2.6.4) to be installed by using a PowerShell command.[49] In other similar cases, attachments of various formats (.zip, .pdf, .iso, .img) delivered the Lokibot, Formbook and Agent Tesla trojans.

Phishing is a *social engineering* method that is used to *trick* a victim into revealing sensitive data, or eventually installing malware such as ransomware. Cybercriminals impersonate legitimate organisations by disguising a website or an email to look like a legitimate one. Phishing emails typically contain malicious attachments or links to malicious websites with drive-by downloads. Phishing websites typically steal account passwords or other confidential information.

With the rise of online shopping, most people rely on courier services such as UPS, DHL, Fedex, and many more. In addition, e-services such as sending invoices through email have also become common. In the same way, threat actors behind massive spam campaigns have followed this, too, and have used these themes extensively as lures to open malicious attachments or click links that would lead to malicious content. Fake delivery notices and invoices were commonly seen with spam campaigns delivering malware.

The CaaS model facilitates the entry into spamming and phishing by making available anything needed to carry out such attacks (Europol, 2014). Email spamming and phishing products and services are widely sold in underground markets by cybercriminals. Databases of email addresses

[48] https://www.kroll.com/en/insights/publications/cyber/monitor/vpn-vulnerabilities-rising-data-exposure-ransomware

[49] https://www.trendmicro.com/vinfo/mx/security/news/cybercrime-and-digital-threats/emotet-uses-coronavirus-scare-in-latest-campaign-targets-japan

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

and social accounts are in high demand. For example, 2.4 million Canada emails cost only US $10, while the same price buys 4.78 million Mexico emails (2021 prices).[50]

Moreover, spam distribution tools and services are available for purchase. Email spamming services range from low-cost solutions of $1-3 US for 10,000 emails (Goncharov, 2015b), $10 US for 1,000,000 emails, up to high-end solutions that charge US $500 US for 1 million emails using a customer database (Goncharov, 2012). Other advertisements promise spamming services to 1000 email addresses for $1.60 (Trend Micro, 2015b) or 20,000 email addresses for $47 and 50,000 email addresses for $95 (Gu, 2013).

1.14 Crimeware - Ransomware-as-a-Service

Several types of malware and hacking tools that can be used to conduct cybercrime operations can be found for sale both in underground markets and in forums on the Dark Web, as well as on the open web. Additionally, cybercriminals have taken this one step further and provide a set of services along with the actual malware. As in the case of legitimate commercial software companies, services such as 24/7 customer support and frequent updates and patches are included in the plan. This model is known as Malware-as-a-Service (MaaS) and is an essential component of the CaaS ecosystem and economy (Europol, 2014).

> “ CRIMEWARE-AS-A-SERVICE:
>
> WE CAN INSTALL YOUR MALWARE IN 1,000 COMPUTERS!
>
> YOU PAY A SMALL FEE PER INSTALLATION!

RATs, trojans, ransomware, keyloggers, spamming tools and even complete botnets can be found at prices that vary per product and service. For example, in 2016, a botnet of 100,000 bots was found for sale on the AlphaBay Dark Web marketplace for $7,500, payable in bitcoin.[51]

Trojans and keyloggers are sold for $1-50; a rootkit that operates in Linux and replaces popular Linux commands (such as “ls” and “find”) can be purchased for $500, a Windows rootkit for $292 and worms and ransomware for about $10 (Goncharov, 2012). However, prices vary greatly. In many cases, advanced packages that also provide technical support and guidance are available at higher prices. As an example, exploit packs are sold for as low as $25, but also for as high as $3,000 per month (Goncharov, 2012; Trend Micro, 2015a). Another example is the Xena RAT malware, which is available in standard packages but also comes in a Gold package that enables crypting services to ensure that the malware will be undetectable (Wilhoit & Hilt, 2015). Other offerings include monthly and yearly subscriptions to malware toolkits. In 2015, buyers could pay $47 US per month for the Fengtian remote access toolkit and $95 US per year for the MBZ remote access toolkit (Gu, 2015). Most expensive RAT toolkits can cost up to $250 US per year (Gu, 2013).

Ransomware, as one of the most popular types of crimeware, is sold in every underground marketplace. For example, Ranion is ransomware that is promoted as a service on the Dark Web. Ransomware-as-a-service (RaaS) means that the tool can be modified by the customer and

[50] https://www.privacyaffairs.com/dark-web-price-index-2021/#8

[51] https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web/

customised to attack specific targets.[52] For Ranion, there are multiple subscription plans available at different prices, the cheapest being $120 US for a month and the most expensive being $900 US for a year, which can rise to $1900 US if the customer includes more features in the ransomware package.[53]

Phishing kits are also a popular crimeware tool, allowing scammers who have no technical knowledge to launch phishing attacks. Many phishing kits are easily accessible and openly offered on the web, with no need to go to the underground market. For example, by searching YouTube, one can easily find more than a hundred different phishing kits for sale or free. Each kit is well presented in the videos, showing its capabilities. Offerings usually include email templates, access to the complex phishing platforms, or even tutorials as part of the package. Some kits are available for free, or with prices ranging from $10-$100.[54]

1.15.1 Pay-per-install (PPI)

A popular method to distribute crimeware and infect computers is the pay-per-install (PPI) service, an instance of CaaS found in underground marketplaces (Europol, 2014). In this business model, PPI service providers distribute a malicious executable (typically provided by customers) and get paid according to the number of successful "installations". An "installation" refers to downloading the malicious file onto a victim's computer and launching it (Goncharov, 2015a). Many of the prevalent malware families in the past have employed PPI services for their distribution (Caballero, 2011).

Prices for such services vary per target country and region. In Europe and the UK, the cost per 1000 installations is $80-130 US, while in the USA the price is slightly cheaper ($40-100 US). In Russia, 1000 installations could cost $100-200 US (Goncharov, 2015b).

1.15.2 Affiliate programme

Ransomware-as-a-Service is very popular in the underground market. Some of these offerings are renting services where cybercriminals who manage to breach the target's network pay a fee to the ransomware author. According to BleepingComputer, only the lowest quality ransomware is offered for rent or sold in this manner.

The most popular and well-known forms of ransomware are actually offered with affiliate programmes. Ransomware gangs usually run private affiliate programmes, where affiliates can submit applications and résumés to apply for membership. Once an affiliate is accepted in the program, they are offered around 70-80% of the ransom payout from the attack, and the ransomware author receives the remaining 20-30%.

This model of distribution was used by over two dozen ransomware-as-a-service operators as they actively sought to outsource extortion attacks to ransomware affiliates. Groups that operate within this programme are associated with high-profile attacks delivering Ryuk, DopplePaymer, Egregor, REvil/Sodinokibi, Netwalker/Mailto, SunCrypt, Clop, Ragnar Locker, Avaddon, DarkSide and many

[52] https://ransomware.fandom.com/wiki/Ranion_Ransomware
[53] https://www.welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices/
[54] https://isc.sans.edu/forums/diary/Phishing+kits+as+far+as+the+eye+can+see/26660/

more. Ryuk affiliates were reported to have collected at least $34 million from a single victim in 2020.[55]

1.16 Data-as-a-Service (DaaS)

Stolen data obtained by illegal operations from various sources are available in almost every underground forum in the world. Dominant products are stolen bank accounts and credit card credentials and copies. Cybercriminals generally exploit two techniques to acquire such information: trojan malware and phishing. However, in the natural world, criminals also deploy ATM skimmers[56] to steal credit card information. In any case, after the criminals gain access to the information that leads to the real assets, they sell it to underground markets or attempt to impersonate the victim in order to withdraw or transfer the funds (Jianwei et al., 2015). Other data include phone numbers, email addresses (see Section 6.15), names, dates of birth and any kind of counterfeit physical documents, such as fake passports, driver's licenses and ID cards (Europol, 2014).

1.16.1 Credit card credentials

Stolen credit card credentials and clones abound in underground markets, although the latter are more risky to use. Prices for US credit cards range from about $20 US for classic US-issued credit card credentials (set of 100) to double this price for Gold, Platinum, or Business US-issued credit card credentials (set of 50). For Canadian credit cards the price is close to $50 US for classic credit cards (set of 50) or Gold, Platinum, Business (set of 35). In these sets, about 15% of the cards in the set are expected to work, otherwise buyers could ask for a refund (Wilhoit & Hilt, 2015; Urano, 2015). In 2021, credit card clones cost from $25 US for a typical VISA or MasterCard with PIN to $240 US for a card that contains a balance up to $5000 US. Credit card credentials cost from $17 US for a USA card with CVV to $65 for an Israeli card with CVV.[57]

1.16.2 Carding

Carding is a form of credit card fraud in which an attacker first steals credit card details and later uses them to buy prepaid gift cards. The holder of the stolen cards, a carder, typically purchases store-branded gift cards using the stolen credit card details. Such gift cards are then used by attackers themselves or further resold in the underground market. The main service offered by carders is thus a collection of prepaid store-branded gift cards. As credit card companies offer customers protection from fraudulent charges, carders make the gift card purchases instantly before the stolen cards are cancelled.

There are several carders available on the underground market. Joker's Stash, the most prominent of them, closed shop recently, in Feb 2021. However, several others continue

[55] https://www.bleepingcomputer.com/news/security/dozens-of-ransomware-gangs-partner-with-hackers-to-extort-victims/

[56] https://en.wikipedia.org/wiki/Credit_card_fraud#Skimming

[57] https://www.privacyaffairs.com/dark-web-price-index-2021/#2

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

business. As per Gemini advisory, such payment/gift cards typically sell at 10% of their value on the underground market.[58]

1.16.3 Bank account credentials - stolen accounts

In the CaaS industry, specialisation is a cherished quality. There are specialised hackers, then there are specialised resellers, and there are yet other specialised liaisons. Typically, a specialised hacker would compromise bank websites and steal user account details. After obtaining such data, one might think that the hackers transfer all the money from those hacked accounts and keep it for themselves. However, such methods are fraught with risks for the hacker, with increased chances of getting caught.

In the CaaS model, instead, things work in groups at multiple levels. Thus, apart from keeping some money for themselves, hackers would typically take several other actions to profit from the hacking operation. One straightforward and highest yield option is to sell such bank account information on the underground market. According to some reports,[59] such account details can be sold for $40-120 (depending on the balance in the account). This delegates the culpability from one hacker entity to several others, making the job tough for law enforcement. The buyers can then further resell the data in smaller sets, making more money. Thus, a single big set of data can end up as smaller sets in the hands of several specialist entities, who can then creatively abuse the stolen data. In addition, stolen bank account information may also be used by hackers to purchase items, create online accounts, apply for house loans, etc.

1.16.4 Non-banking account credentials - stolen accounts

Credentials for various online accounts are also available for sale. Apart from banking accounts, which are the most prevalent, credentials for several popular platforms can be illegally acquired. Cybercriminals steal such account information and sell access to their buyers. Hacked accounts include PayPal, Netflix, Spotify, Origin, Beats Music, Hulu Plus, Dish Network Anywhere Luminosity, Sirius Satellite Radio, etc., and are available for as little as $20 US each. As long as the compromised users do not change their passwords, buyers can use the platforms at very low prices (Wilhoit & Hilt, 2015; Urano, 2015). In 2021, stolen accounts have become a little more expensive, up to prices that range from $35 to $80 US.[60]

1.16.5 Phone number databases

Databases of phone numbers are available for sale on the underground market. Such databases, along with other PII information, could be very useful to cybercriminals for various illegal operations and scams. Phone number lists are typically categorised per town or city. For mobile phone numbers, prices range from $290 US for a small town to $1236 US for a big city (Mercês, 2014). Similarly, for home phone numbers prices range from $317 US to $1931 US (Mercês, 2014).

An instance of such a database is the Japanese underground site called "JPON EXTREME". This database offers its users a total of 600 million telephone records, collected since 1993, along with the owners' names and addresses (Urano, 2015).

[58] https://geminiadvisory.io/gift-card-shop-breached/
[59] https://www.privacyaffairs.com/dark-web-price-index-2021/#5
[60] https://www.privacyaffairs.com/dark-web-price-index-2021/#5

Recent data scraped from Facebook and posted on the Dark Web, also included millions of phone numbers. The sheer number of phone numbers leaked prompted security researcher Troy Hunt to add a functionality to his website HaveIBeenPwned, to allow victims to search by their phone numbers to verify if their numbers have been leaked.[61]

1.16.6 Fake documents - identity theft

In many cases, cybercriminals need to provide an ID. For example, to open an account that will send/receive money, the cybercriminal needs to provide an ID document, usually a passport, as well as scanned copies of several types of documents such as utility invoices, bank statements, etc. Scanned document copies or fakes are available as a CaaS product and sell very well in underground markets. Similar services include reworking of scanned documents.

Prices range from $1-5 US for a European passport scan to $5-28 US for a document or a credit card rework service (Goncharov, 2015a). A Canadian, UK or US passport scan costs $25-30 US. Fakes can be found at higher prices and depend on the document quality. A fake Canadian, UK or US passport or driver's license costs $630-780 US (Wilhoit & Hilt, 2015).

In 2021, a Minnesota driver's license scan costs $20 US, a New York driver's license scan costs $80 US and a Russian passport scan costs $100 US. In the case of physical documents prices are higher. A fake US Green Card costs $150 US, an American ID costs $50-185 US, a European national ID costs about $120 US, a European passport costs $1500-4000 US and a US driver's license costs $100 US.[62]

1.16.7 PII querying

Personally Identifiable Information (PII) refers to the information that can be used to identify a specific individual. Usually such information is private and sensitive. Some examples of personally identifiable information are:

- Identity: Name, date of birth
- Contact information: Address, phone number, email address
- Professional information: Job, company, position
- Administrative documents: Passport number, driver's license, social security number
- Health records

PII could be used to create fake identities in the victim's name, including the creation of passports for criminal purposes. Therefore, protection of PII is critical. Different countries have different laws for protecting PII. For example, in the European Union, the GDPR dictates the policies surrounding protection of PII. It even includes entities that by themselves do not contain personal information but can still be used to deduce someone's identity (such as IP address, geolocation, etc.).

Cybercriminals who have gained access to databases of national services, such as vehicle registration plate databases and national health databases, offer PII-querying services in underground markets (Trend Micro, 2015a). In these platforms any type of stolen PII can be

[61] https://www.troyhunt.com/the-facebook-phone-numbers-are-now-searchable-in-have-i-been-pwned/
[62] https://www.privacyaffairs.com/dark-web-price-index-2021/#7

acquired for just a few dollars. Interestingly enough, in some cases, the individuals who were found guilty of selling access to national databases were government employees (Trend Micro, 2015a)! On English-language Dark Web marketplaces, the price range for PII of US citizens is typically $1 to $8 US.[63]

1.17 Serial keys - pirated software

Many advertisements can be found in various websites and forums that illegally sell serial and activation keys for popular software packages. Such serials are fully functional and can be obtained at prices significantly lower than the officially suggested retail prices. However, the sources of such keys are in most cases illegal and police have been issuing charges for copyright infringement and money laundering.[64]

Prices for serial keys of Microsoft products, such as Windows 10 Pro, Office 2016 and Windows Server, as well as other popular programs like Adobe® Photoshop and AutoCAD, are often less than $10 US (Goncharov, 2012).

1.18 Social boosters - friends and “likes” for purchase

Social boosters are tools that help users to gain more attention on social media platforms. By using a booster, someone can buy “likes/views” or “followers/friends”. In platforms other than social media, “boost” can be measured in terms of downloads or votes in order to acquire an award.

> “Would you like some friends to “like” your web page? Easy-peasy!
>
> Hire-a-Friend and purchase some Likes now!

In underground forums, users can find services that promise to boost the popularity of their accounts, e.g. in Sina Weibo, one of the biggest social media platforms in China with hundreds of millions of monthly active users. Advertisements show that 10,000 followers could cost from $7 to $161 US, while 1000 comments can be bought at prices that range from $8 to $63 US (Gu, 2015). In 2021, 1000 followers or likes in Instagram cost $5 US, while 1000 retweets in Twitter cost $25 US.[65]

1.19 Web traffic - visitors

Criminals who have access to web traffic (i.e. they control a web site with a large number of visitors) may put it for sale in the markets or use it for their own malicious purposes. Traffic can be used for a variety of aims, such as for blackhat search engine optimisation (SEO) or to increase the number of downloads and visits on a website. Traffic can be gained from exploited websites where visitors unknowingly request additional URLs that belong to the cybercriminals. Hackers who have

[63] https://www.itproportal.com/features/pricing-of-goods-and-services-on-the-deep-dark-web/
[64] https://tarnkappe.info/windows-10-lizenzkeys-staatsanwaltschaften-verschicken-vorladungen/
[65] https://www.privacyaffairs.com/dark-web-price-index-2021/#5

acquired access to such vulnerable websites can direct their visitors to generate traffic to their own network locations, thus increasing the number of downloads and hits.

Prices for such services depend on the kind and the origin of the traffic for sale. Traffic and downloads from business-oriented visitors are more expensive than those from ordinary visitors. Moreover, traffic originating from European countries and the US is more expensive than traffic originated from other countries. In any case, prices are generally low: for example, 1000 visitors from premium countries can cost about $5 US in Russian underground markets (Goncharov, 2012), while someone could find the same price in the Chinese markets for a plan of 10,000 visitors per day. At higher prices, buyers can get 500,000 visitors per day for $462 US (Gu, 2015).

1.20 Cybercriminal business, marketing and messaging

Cybercrime has grown to be increasingly organised and sophisticated. Profit-driven cybercrime functions as a profitable industry with business-like elements, structure, and governance. The elements of today's cybercriminal business include specialisation, professionalisation, the growth of virtual marketplaces and the organisation of cybercriminals into groups that resemble legitimate firms and have even adopted business practices, such as marketing and PR (Lusthaus, 2018b). Cybercriminals do business in varied ways, some of which include adopting modern as-a-service business models.

Cybercriminals are increasingly specialised in certain roles. Some of the roles, such as hacking, are for more tech-savvy cybercriminals, while some are for more business-minded individuals. This specialisation has allowed cybercriminals to benefit from the skills of others. Specialisation also drives the industry and gives room for different types of people to get involved in cybercrime. (Lusthaus, 2018b). For instance, in Europe, there has been a rise in less tech-savvy cybercriminals in the context of CaaS solutions, and criminals are able to hire specialists with particular skills, such as malware coding or malware distribution (Europol, 2020).

Cybercrime has also become increasingly professional (Europol, 2020), and for many cybercriminals cybercrime is a full-time job. The professionalisation phenomenon of cybercrime embraces both the increasingly professional nature of cybercriminals and the increasingly professional business-like way cybercrime is carried out (Lusthaus, 2018b).

Cybercriminals have similar organisational structures to legitimate firms. These structures depend on the focus of the criminal group, and they vary from small "crews", such as cashing out groups, to large enterprises. Some of these groups also have a strong physical presence, and may even operate from physical office spaces (Lusthaus, 2018b; Lusthaus & Varese, 2017).

Cybercriminal groups have adopted different business practices, such as practices related to marketing and customer experience. These include shopping experiences similar to legitimate businesses, including virtual shopfronts operating like regular online stores, and even refunds after customer complaints. Some cybercriminal groups invest in marketing and even have separate marketing departments and customer support functions. (Lusthaus, 2018b). For instance, in Europe, ransomware attackers have engaged in public relations activities: some even conduct their own PR campaigns and release statements, like the Maze ransomware group during the Covid-19 pandemic (Europol, 2020). In addition, lone operators might engage with others by using freelance services, even for marketing purposes (Lusthaus, 2018b).

The Hellenic Police has observed a recent example of cybercriminal business structures and practices that is related to the excessive number of complaints recorded about cyber financial crimes, such as investment fraud schemes, during the last two or three years. Based on exhaustive investigations by the Hellenic Police authorities, they have concluded that these investment companies have specific business structures (customer service, marketing department, human resources dept., legal dept., managers, etc.) and follow tactics to appeal to customers and convince them to invest in the financial products they promote, promising them lavish returns. According to ex-employees' testimonies, the criminal groups apply high-pressure psychological marketing tactics and methods, so as not to give the customer the opportunity to evaluate the services offered. After the customer has invested money, they are not given the option to withdraw the returns or even the initial capital invested.

Business-like ways of operation also include the use of business models similar to those of legitimate software companies. For instance, the malware business has become increasingly advanced. Some malware businesses operate through a licensing-based business model (Lusthaus, 2018b).

Europol (2020) has observed an increase in subcontracting and cooperation between cybercriminals, for instance in malware, infrastructure and money laundering activities. One of the most notable examples is the relationship between Emotet, Ryuk and Trickbot: "Similarities in how criminals behind the trio, Ryuk ransomware, Trickbot and Emotet malware, operate suggests that criminals across different attack approaches could either belong to the same overall structure, or that they are becoming smarter at cooperating with each other" (Europol, 2020).

Marketplaces and forums of cybercriminals have been and continue to be important to the cooperation and development of profit-driven cybercrime, even if law enforcement interactions have weakened their effectiveness (Lusthaus, 2018b). They provide a place to sell products and services, network, share information, and look for partners with other specialisations, and there is a level of governance in place to facilitate doing business. However, cybercrime markets go beyond large marketplaces and forums, and smaller groupings are common (Lusthaus, 2018b). Even if a cybercriminal uses forums to find partners or buyers, the deals are often conducted via private messages and channels.

Marketplaces and forums include Dark Web marketplaces and Dark Web hacker forums, which are accessible via the tor browser, and surface web hacker forums (see section 3.3). The promotion of the marketplaces happens via word-of-mouth. The mechanisms built to facilitate business in the marketplaces include the use of confirmed vendors: services provided by a vendor can be rated, in a similar way to eBay or other online marketplaces.

There is always a risk of being scammed by strangers, and anonymity poses challenges to the cooperation between cybercriminals, so building trust through reputation and appearance is important (Lusthaus, 2018a; Lusthaus, 2018b). Marketing of individuals in Dark Web hacker forums happens mostly via username recognition, because the forums are anonymous—you are the username you carry. A user might build a reputation for the username and have the same username on multiple forums. If the user posts material that is generally considered to be good, their credibility on those sites goes up. Some forums also have mechanisms similar to a reddit upvote system, but instead rating users.

In the future, cybercriminal business will continue to evolve. For instance, the use of AI offers criminals new ways to facilitate and improve their attacks and create new business models, such as AI-as-a-Service, which will continue to lower the entry barriers to criminal activities (Europol, 2020).

1.21 Underground forum access

Forums on the web are an old phenomenon. However, this old phenomenon is one that is the most popular among hackers on the underground market. Forums are a platform for both experienced and new hackers to share cybercrime knowledge, experiences, and of course to buy/sell illegal items. However, in a world of anonymity and mistrust, it is a challenging task to conduct business with strangers. How can both parties trust each other in a deal of illegal activities? Paradoxically, in a dark anonymous world, more information is the key to success. In the world of underground forums, older means more respected. An old forum indicates that it has stood the test of time, thereby increasing trust. Similarly, an old user indicates experience and thereby more worth.

How does a new user join such forums though? Users can register by sending a registration request to the administrator of the forum. Depending on the type of the forum, a new user may be allowed to join with selected posts available only to “high rank” users. There are other forums that are “invitation only”.

Let us now look into more detail as to how both parties (buyer and seller) of a transaction on a forum can trust each other. Forums typically provide a status mechanism for users. A user with quality posts, valuable contributions/helping posts for other users of the forum, earns more points over time rising through the ranks. There are several evaluation criteria provided by forums to evaluate the status of a user: date of joining, number of posts over a period of time, previous transactions conducted, level of involvement in “forum life”, etc. A higher rank user automatically is respected and trusted more. Similarly, other users may also vouch for some user, a sure sign of legitimacy. Then there are forums that make users pay to rise through the ranks, the idea being that such payments would filter out scammers and law enforcement officials. On the other hand, any undesirable activities, or inactivity, on the part of users immediately earns them the rank of a “leecher” or “lurker”. Such users can eventually get banned from forums, thereby depriving them of opportunities to gain knowledge or make profit. Finally, some forums provide “VIP” status to certain users, based either on payment of a fee or on their seniority status. A “VIP” status can entail several additional benefits, including access to “restricted content” or escrow services during transactions, providing dependability.

At the time of a transaction, both the seller and buyer would then be able to view the other party's status, forum activity and history. They can judge credibility based on several factors, including reviews by other forum members or previous reported problems

Forums are undoubtedly the most popular means of conducting transactions on the Dark Web. Forums provide something more to hackers than being mere transaction platforms. They provide a sense of community to hackers, where they can share their knowledge, experiences of run-ins with law enforcement officers, mistakes made by other members who got arrested, or simply a sense of fraternity—even to raise money for fellow members' cancer operations.[66]

There are, however, some forums that also share data dumps and credential lists for free. The quality of the free dumps can be questioned, but most often all of them circulating around the web seem to come from a singular source, meaning that the poster might not be the original leaker of the data file. It would seem that the motivation behind sharing them for free might be as simple as reputation farming. Usually, the forums hosting these data dumps reward active people, in the form of internet fame governed by a voting system. If the user posts potentially interesting or useful material, such as data dumps, they might be rewarded with a VIP membership, gaining further access to restricted parts of the forums.

There are also some deep web hacker forums, which might grant access to a person if they have a high reputation on some other platform, instead of making them pay the usual entrance fee.

To summarise, it seems that today there exist a variety of cybercrime products and services provided using the "Cybercrime-as-a-Service" business model. Although all of them are important (i) to understand, and (ii) to mitigate, if we were to select three of the most significant ones they would seem to be:

- Cryptocurrencies - including laundering and tumbling
    - These enable cybercriminals to send and receive money (almost) anonymously
- Bulletproof hosting
    - This enables cybercriminals to host their services (and conduct illegal activities) without any (at least immediate) danger of being taken down
- Crimeware and ransomware as a service
    - This enables non-technical criminals to use highly sophisticated technical tools that are necessary for their illegal activities

2 Trends and Correlations in the Cybercrime Landscape

As so far discussed, there are multiple technical as well as human drivers that enable cybercrime: like information technology (IT) itself, it is an ever-evolving field. As innovation in the IT sector generates new solutions and new technologies, criminals continuously find numerous ways to exploit them, often for financial gain.

[66] https://www.digitalshadows.com/blog-and-research/forums-are-forever-part-3-from-runet-with-love/#

When we consider trends in cybercrime, they have, through the years, followed the evolution of the IT sector. In the interest of focus, we will study the latest occurring trends in the field based on statistics derived from F-Secure data (F-SECURE, 2018), expert knowledge, as well as open-source intelligence.

The operational models of cybercriminals go through continuous development, driven by the emergence of new technologies or new prevalent vulnerabilities. Some of the criminals themselves are capable of significant innovation; hence, they can become the enablers of new operational models with new exploits and tools. Such tools may, in turn, be shared with the rest of the cybercriminal community, driving a change throughout the field. Some new technologies, such as the cloud, enable new operational models and techniques for cybercriminals of all levels.

2.1 Service models

In recent years, as the adoption of different cloud-based services has increased drastically, new service models have appeared and gained popularity over the traditional on-premises model. The value of such service models has been realised for criminal use cases and so adopted by the criminals in cyberspace.

This has been visible in different crime-as-a-service models such as:

- Hosting services
- Pay per install
- Cryptocurrency laundering
- Ransomware-as-a-service

The popularity of different cloud-based service models has given rise to many free and low-cost hosting providers that are under less pressure from the public to know their customers, as opposed to big well-known entities. This has made cloud hosting services available to cybercriminals, while many of the service providers look the other way.[67] In February 2021 Netskope estimated that 61% of malware is delivered via cloud, essentially hosted in various cloud services.[68] Later, in July 2021, cloud-hosted malware grew to 68%. The majority of malware is hosted and delivered via cloud storage apps (66.4% in July).[69]

Even instant message applications, such as discord, have been used to distribute malware.[70]

Nearly two thirds of ransomware incidents in 2020 were estimated to be related to a Ransomware-as-a-service (RAAS) platform.[71] RAAS has been available in the darknet since 2016[72] and has seen widespread popularity ever since. It is likely that RAAS is one of the major contributors to the prevalence and growth of ransomware in the last decade.

[67] https://blog.malwarebytes.com/cybercrime/malware/2019/01/hosting-malicious-sites-legitimate-servers-threat-actors-get-away/
[68] https://resources.netskope.com/cloud-reports/cloud-and-threat-report-february-2021
[69] https://resources.netskope.com/cloud-reports/cloud-and-threat-report-july-2021
[70] https://www.zscaler.com/blogs/security-research/discord-cdn-popular-choice-hosting-malicious-payloads
[71] https://www.group-ib.com/resources/threat-research/ransomware-2021.html
[72] https://www.crowdstrike.com/cybersecurity-101/ransomware/ransomware-as-a-service-raas/

2.2 Malware

Malware is one of the key tools in a cybercriminal's arsenal as malware continues to evolve to remain relevant. Recently, there have been many significant observable trends in the cybercrime malware landscape, but ransomware has probably been the most damaging of them all and poses a big risk to individuals and organisations.

2.2.1 Ransomware

Malware in general has seen tremendous growth over the last decade and ransomware can be considered as the most prevalent malware type in the wild, most often used by financially motivated cybercriminals. According to a Coalition cyber insurance claims study from H1 2020, 41% of all insurance claims were due to incidents involving ransomware (Coalition, 2020).

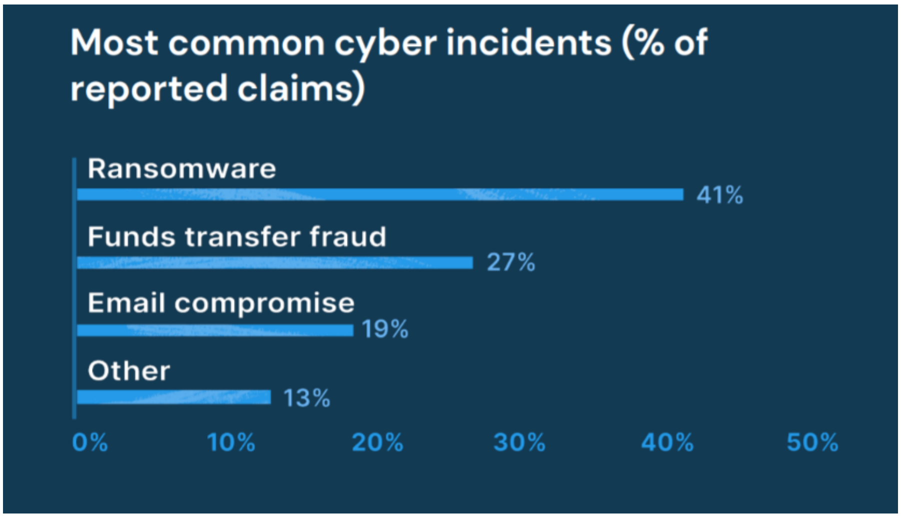


Figure 2: Insurance claims of cyber incidents (Coalition, 2020)

Note that ransomware, in addition to its prevalence, is a particularly damaging and visible type of malware. That is probably why it is at the top with 41% as seen in the figure above. Ransomware as a malware type has seen constant annual growth over the last decade and, according to a Bitdefender report, ransomware in terms of volume saw an annual growth of 715% from 2019 to 2020 (Bitdefender, 2020).

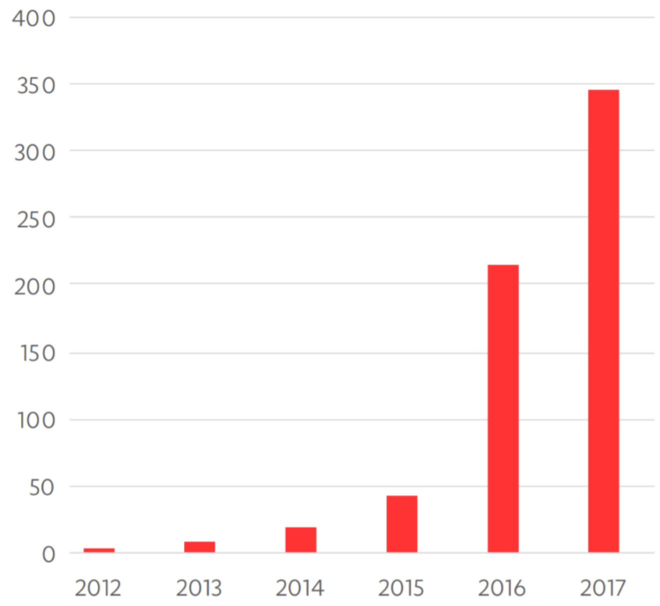


Figure 3: Number of unique ransomware families/variants (F-SECURE, 2018).

Similar growth had already been seen in previous years, in both ransomware variants and their volume, as covered by the F-Secure ransomware report from 2018.

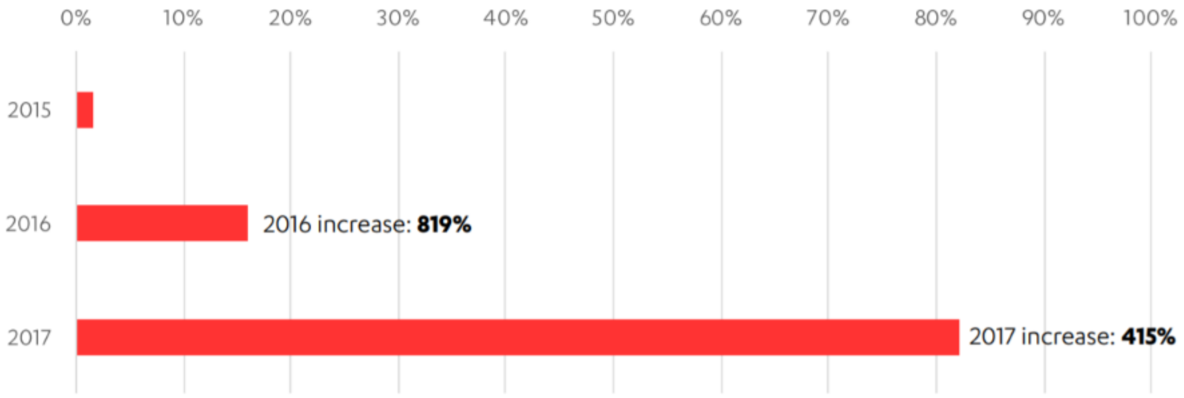


Figure 4: Number of detection reports per year based on percentage of total # of ransomware detections from 2015-2017 (F-SECURE, 2018)

Studying F-Secure endpoint protection metrics, an over 300% growth in detected ransomware from August 2020 to August 2021 has been underlined. In addition to that, in a Bitdefender threat landscape paper from 2020, an increase of 485% from 2019 to 2020 was also noted (Bitdefender, 2020b).

It is clear that the prevalence of ransomware continues to grow, in terms of both new variants and volumes. In addition to the prevalence and rising volumes of ransomware, an upwards trend is

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

observed in ransomware payments.[73] Ransomware groups are known to assess the potential financial gain based on the victims' capability to pay, and to prefer bigger victims. The maturing techniques and tactics may very well manifest in an increasing trend in the size of ransom demands and payments.

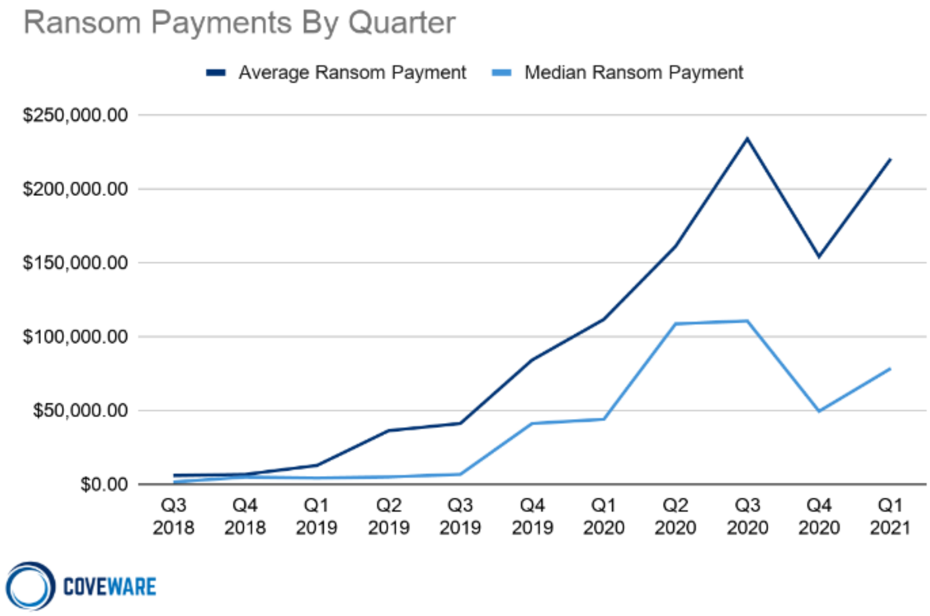


Figure 5: Amount of median & average ransom payments by quarter in USD (Coverware)[74]

2.2.2 PowerShell

PowerShell has seen significant use by cybercriminals in network breaches. In 2016, PowerShell was seen in more than a third of cyberattacks[75] and has since experienced steady growth. According to McAfee threat report, PowerShell malware grew by 208% from 2020 Q3 to Q4 and since 2019 Q4 from roughly 200 thousand to 12.5 million in 2020 Q4, over 6100% growth.[76]

[73] https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
[74] https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound
[75] https://www.computerweekly.com/news/450281204/Windows-PowerShell-tied-to-more-than-a-third-of-cyber-attacks
[76] https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

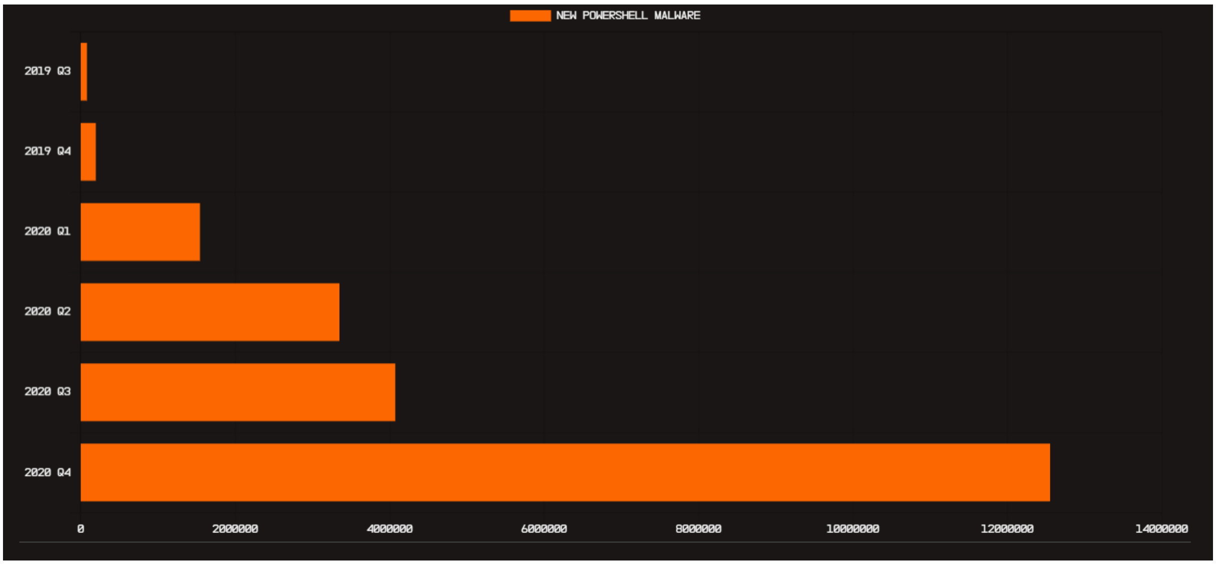


Figure 6: Numbers and growth of new Powershell malware in 2019 and 2021 as observed by McAfee

2.3 Communication methods

Information technology naturally provides international communication capabilities for people, including cybercriminals. Often criminals prefer to stay anonymous on the internet for obvious reasons. There have been many options for communication throughout history but increasing public knowledge of surveillance has raised more concerns about privacy and operational security and made people more aware. New privacy-focused technologies have entered the market and gained popularity in all types of use cases.

2.3.1 Tor

Since its launch in 2002 the communication avenues and opportunities for initial contact have moved largely into the tor network. Today tor is the preferred protocol, because of its anonymous nature (Section 3.5). Despite many efforts by nation states to monitor and reduce the anonymity of tor, the network remains popular among cybercriminals and is also used in other instances, such as hiding the origin of a cyberattack. Different types of hidden forums and marketplaces provide a platform for criminals to exchange information and to network with other like-minded people.

Further conversations between individuals often move to various chat applications and protocols that (i) are relatively well known, (ii) are considered secure, (iii) support anonymity, and (iv) are rarely hosted by organisations willing to comply with law enforcement.

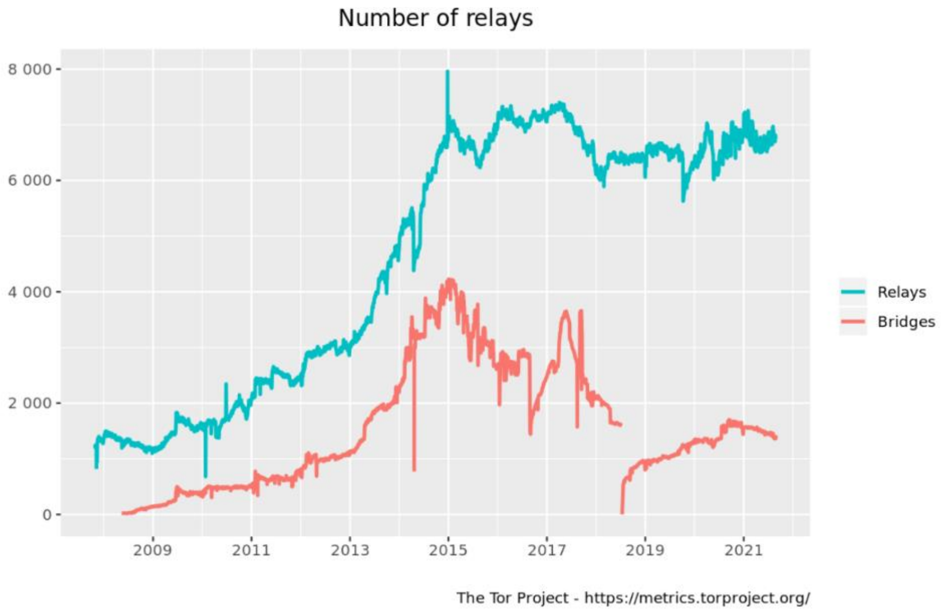


Figure 7: Number of tor relays & bridges since 2008

Tor network statistics (at the time of this writing) from torproject.org highlight steady growth in the infrastructure and adoption of the protocol up to 2015. According to MIT, the number of daily unique users was around 2.5 million in 2015,[77] since when the infrastructure growth has stagnated. The upturn in growth trend from 2013 until 2015 could be attributed to the global surveillance disclosure by Snowden, when the amount of surveillance conducted became known to the public and the effectiveness of the tor network in terms of keeping anonymity & privacy took on added value.

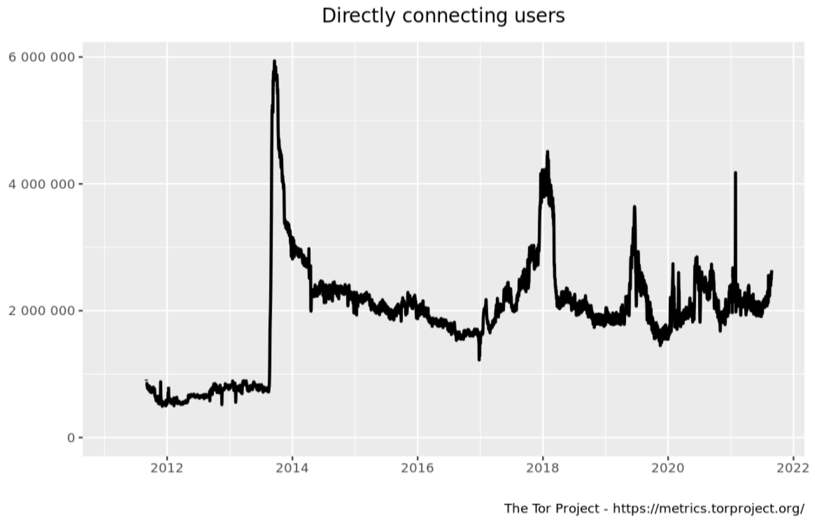


Figure 8: Number of directly connecting users

[77] https://news.mit.edu/2015/tor-vulnerability-0729

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

As regards the amount of directly connecting tor users, the long-term trend is upwards since the beginning of data collection. It should be noted that the connection metrics also include short-lived high-volume botnets and other automated structures that have been developed to use tor.

2.3.2 Email

Email has been one of the key tools in the cybercriminals' arsenal for a long time, almost since its inception. The use of email and email addresses is a fundamental part of the information technology business and still one of the key ways to communicate with other people. Apart from this main purpose, additional applications and systems have been built on top of email and it is the *de facto* requirement for registering a personal account in many services online. Multiple privacy-oriented email services have launched and gained popularity in the last decade. One example is "protonmail", which launched in 2014 as an end-to-end encrypted email service and in 2017 became available in the tor network.

Protonmail is one of many private and secure email services that are also used by cybercriminals. Since its launch in 2014, protonmail has gained 20 million registered users until the end of 2019 and over 50 million during 2020.

2.3.3 Instant messaging

In addition to email, cybercriminals use other communication methods online. A large portion of business happens in private encrypted channels out of sight. Throughout the decade, cybercriminals have used applications like Jabber to communicate, but with new apps and technologies emerging, they are also being increasingly used by criminals. Applications like Telegram and Discord provide a useful instant messaging feature set as well as a strong focus on privacy. This is lucrative for the cybercriminals and they have been quick to use such applications. Telegram allows for establishing groups in the messaging application; in 2020 it was estimated by Cloudsek that 30-40% of these communities in Telegram offered some sort of hacking/cybercrime services, often advertised as "ethical".[78]

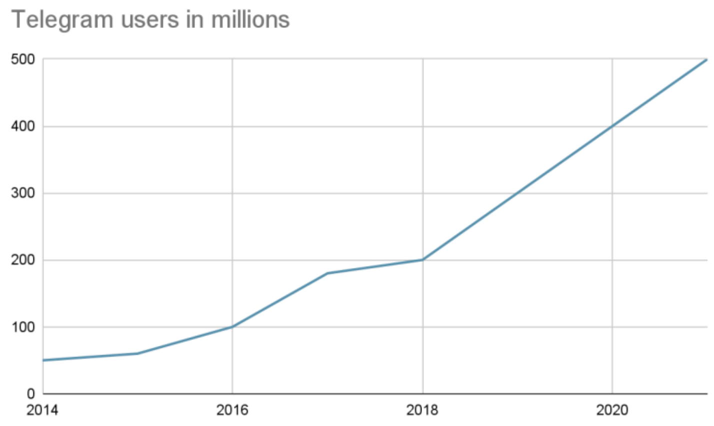


Figure 9: General Telegram popularity has been in a steady growth[79]

[78] https://cloudsek.com/the-rise-of-cybercrime-on-telegram-and-discord-and-the-need-for-continuous-monitoring/
[79] https://siteefy.com/telegram-statistics/

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

The increasing popularity and the feature set of Telegram are likely to increase its use in criminal cases in the future. Instant messaging in mobile applications increases the mobility and speed of cybercriminals in general, so there are some benefits over using full desktop or laptop computers for communications and accessing a market. Privacy-focused applications are here to stay and they will be increasingly popular in the cybercrime field, too.

2.4 Monetisation

Most often than not, cybercriminals are financially motivated and looking to get paid. In traditional crime, cash is great, but for cybercrime there are better alternatives. Cybercriminals often resort to the darknet markets for selling and buying goods and services, because of the anonymity and the communities of like-minded people. Since the inception of cryptocurrencies, they have become the main currency of the underground.

2.4.1 Darknet/DarkWeb

The darknet[80] is a constantly evolving ecosystem and the trends within are driven by multiple factors, whether that be new technologies, vulnerabilities or law enforcement actions and legislation.

In the darknet, there are often listings of malware and tools that are used in cyberattacks against organisations. In a study from 2018, Bromium estimated that over a two-year period (since 2016), the quantity of offerings with potential impact on organisations' security had increased by 20%.[81]

These offerings with impact potential include:

- Targeted malware
- Enterprise-specific DDoS services
- Corporate data for sale
- Brand-spoofing phishing tools

Out of all the investigated listings related to digital products (43% of all listings), 60% had direct potential to cause a harmful impact on organisations' cybersecurity, while 15% of digital offerings were considered to have potential for reputational impact.

In terms of general interest in "darknet", a google search trend shows that the darknet searches peaked around 2017 and have been in a steady decline. Searches for "tor" are a lot higher in volume but the trend is similar.

[80] https://en.wikipedia.org/wiki/Dark_web
[81] https://www.bromium.com/wp-content/uploads/2019/06/Bromium-WoP-Behind-the-Dark-Net-Black-Mirror.pdf

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

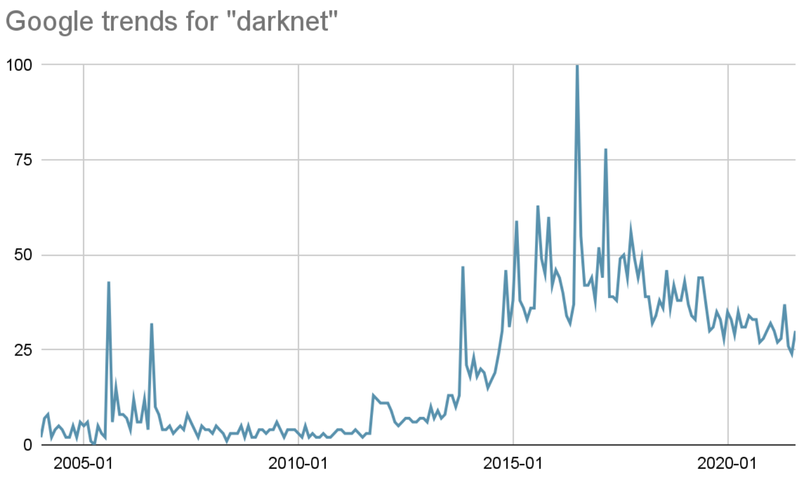


Figure 10: General Telegram popularity has been in a steady growth

2.4.2 Cryptocurrencies

Cryptocurrencies are the go-to currency of cybercriminals today. The relative ease of use, anonymity and automation make crypto a favourable option for cybercriminals.

The popularity of bitcoin has been steadily increasing globally, for both legitimate and illegitimate use cases. The daily transaction numbers highlight its rising popularity over a long period of time.

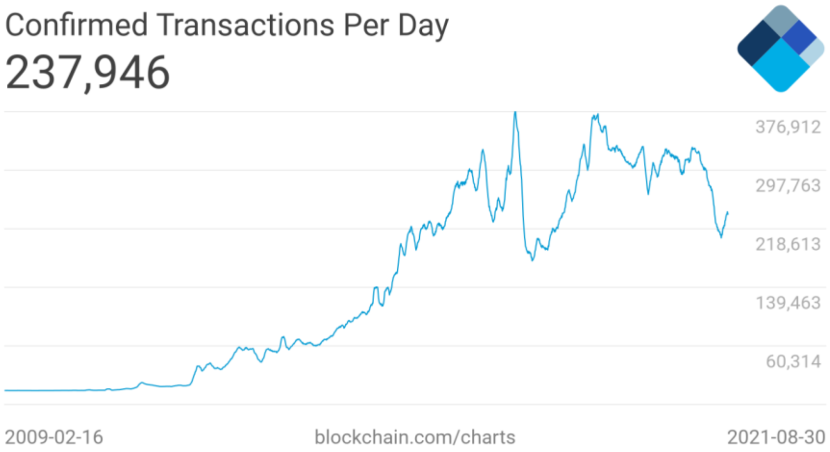


Figure 11: Bitcoin daily transactions 30 day average (Blockchain.com)[82]

[82] https://www.blockchain.com/charts

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.

In 2018, Europol estimated that about US$ 5.5 billion USD worth of money was laundered by criminals through cryptocurrencies.[83]

In 2019, the amount of cryptocurrency usage by criminals increased by over 300% and peaked at about 2% of total transfer value of cryptocurrencies.[84] While the number of criminal transfers is lower than 2019, the trend is upwards and is a significant amount of money ($10 billion in 2020).

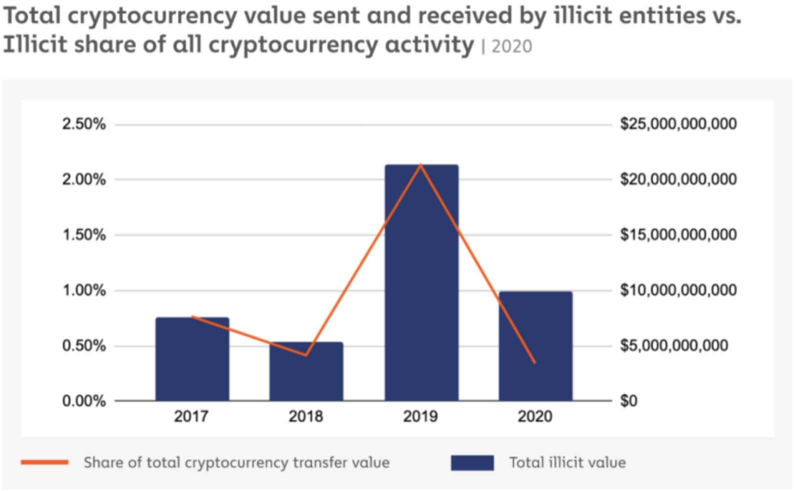


Figure 12: Illicit crypto transfers (chainanalysis)[85]

While cryptocurrencies are an important intermediate currency, cybercriminals often intend to exchange these for native currencies and launder the money.

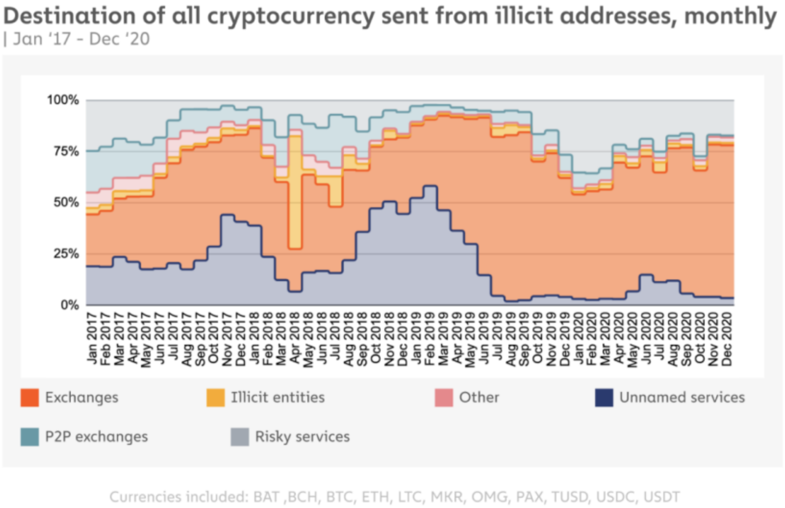


Figure 13: Illicit cryptocurrency transfer destinations by type (chainanalysis)[86]

[83] https://www.businessinsider.in/tech/criminals-in-europe-are-laundering-5-5-billion-of-illegal-cash-through-cryptocurrency-according-to-europol/articleshow/62888250.cms

[84] https://go.chainalysis.com/2021-Crypto-Crime-Report.html

[85] https://go.chainalysis.com/2021-Crypto-Crime-Report.html

[86] https://go.chainalysis.com/2021-Crypto-Crime-Report.html

In 2020 most of the illicit crypto transfers were into different mainstream exchanges. Exchange platforms are safe options for storing and exchanging currencies, although most of these are centrally managed and under some jurisdiction with laws against money laundering. New laws proposed in the EU[87] intend to make centralised exchanges riskier for illicit transfers, a share of these transfers is likely to move into other places, such as P2P exchanges, or other services with risks other than law enforcement action.

2.5 Offerings in cybercrime forums

> “84% INCREASE IN THE NUMBER OF USERS IN THE RUSSIAN-SPEAKING FORUM.
>
> *Elias Koivula*

Akyazi et al. (2021) measure the proliferation of the supply and demand for cybercrime-as-a-service in underground fora. They use a machine learning approach to classify each post in the appropriate category. They report that crimeware-as-a-service seems to be very strong with 15.6% of the offerings. 12.6% of the offerings are related to cache-out. The crimeware-as-a-service includes “botnet as a service”, “reputation escalation as a service”, and “traffic as a service” at 22%, 24%, and 18.5% of the total cybercrime-as-a-service offerings. In their experiments they did not see any significant change in the cybercrime-as-a-service offerings. On the other hand, they report that such a change may be happening in other fora which they did not include in their study.

On the other hand, Koivula (2021) found that the number of users in a Russian-speaking forum they studies had increased by 84% between February 2019 and November 2019. At the same time, the number of posts had increased by close to 25% from 130,040 to 162,470.

Finally, Buil-Gil at al. (2021) found that Denial of Service attacks have increased by 28% in the UK between May 2019 and May 2020. They also found that in the same period cybercrime in the UK has increased by an average of 43%.

3 Summary

In this document, we have presented the landscape for Cybercrime-as-a-service. We notice that there is a wide variety of such services offered that include (i) 1.1 Cryptocurrency laundering and tumbling, (ii) 1.2 Bulletproof hosting, (iii) 1.3 Tutorials, training and consulting, (iv) 1.4 Hacking-as-a-Service, (v) 1.5 Coding/Programming-as-a-Service, (vi) 1.6 Crypting - obfuscation, (vi) 1.7 Distributed denial-of-service (DDoS) attacks/Reflection attacks (DRDoS), (vii) 1.8 SMS flooding and spamming, (viii) 1.9 Escrow/Garant/Treuhand, (ix) 1.14 Email spamming and phishing, (x) 1.14 Crimeware - Ransomware-as-a-Service, (xi) 1.17 Serial keys - pirated software, (xii) 1.18 Social boosters - friends and “likes” for purchase, (xiii) 1.19 Web traffic - visitors, (xiv) 1.20 Cybercriminal

[87] https://www.reuters.com/technology/eu-tighten-rules-cryptoasset-transfers-2021-07-20/

business, marketing and messaging. Although it is difficult to estimate trends, we see that several of these services have increased or at least have stayed the same over the past few years.

It is evident that cybercrime is a growing business with new actors and groups entering the field, new marketplaces spawning in the darknet to replace old ones, and new services and products emerging to counter new defences.

Ransomware remains the most impactful malware and is generally considered the biggest risk facing organisations worldwide. Ransomware authors have adapted and evolved over time to use new techniques to maximise damage and potential financial gain as global ransomware volumes still continue to grow exponentially.

This project has received funding from the European Union’s Horizon 2020 research and innovation program under grant agreement No 883543.

References

Akyazi, U., van Eeten, M. J., & Ganan, C. H. (2021). *Measuring Cybercrime as a Service (CaaS) Offerings in a Cybercrime Forum*. Workshop on the Economics of Information Security.

Bitdefender (2020). *Mid-Year Threat Landscape Report 2020*. Available at: https://www.bitdefender.com/files/News/CaseStudies/study/366/Bitdefender-Mid-Year-Threat-Landscape-Report-2020.pdf

Bitdefender (2020b). *2020 Consumer Threat Landscape Report*. Available at: https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf

Buil-Gil, D., Miró-Llinares, F., Moneva, A., Kemp, S., & Díaz-Castaño, N. (2021). Cybercrime and shifts in opportunities during COVID-19: a preliminary analysis in the UK. *European Societies, 23*(sup1), S47-S59.

Caballero, J., Grier, C., Kreibich, C., & Paxson, V. (2011, August). Measuring pay-per-install: the commoditization of malware distribution. In *Usenix security symposium* (Vol. 13).

Coalition (2020). *Cyber Insurance Claims Report*. Available at: https://info.coalitioninc.com/rs/566-KWJ-784/images/DLC-2020-09-Coalition-Cyber-Insurance-Claims-Report-2020.pdf

Europol (2014). *Internet organised crime threat assessment*. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2014

Europol (2020). *Internet organised crime threat assessment*. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020

F-SECURE (2018). *The changing state of Ransomware*. Available at: https://techfromthenet.it/wp-content/uploads/2018/05/fsecurepressglobal.files_.wordpress.com_2018_05_ransomware_report.pdf

F-SECURE (2020). *Attack Landscape H1 2020*. Available at: https://blog.f-secure.com/podcast-mikko-hypponen-covid-19/

Goncharov, M. (2012). *Russian Underground 101*. Trend Micro. Available at: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-101.pdf

Goncharov, M. (2015a). *Russian Underground Revisited*. Trend Micro. Available at: https://www.trendmicro.de/cloud-content/us/pdfs/security-intelligence/white-papers/wp-russian-underground-revisited.pdf

Goncharov, M. (2015b). *Russian Underground 2.0*. Trend Micro. Available at: https://documents.trendmicro.com/assets/wp/wp-russian-underground-2.0.pdf

Goncharov, M. (2015c). *Criminal Hideouts for Lease: Bulletproof Hosting Services*. Trend Micro. Available at: https://documents.trendmicro.com/assets/wp/wp-criminal-hideouts-for-lease.pdf

Gu, L. (2013). *The Chinese Underground in 2013*. Trend Micro. Available at: https://documents.trendmicro.com/assets/wp/wp-the-chinese-underground-in-2013.pdf

Gu, L. (2015). *Prototype Nation: The Chinese Cybercriminal Underground in 2015*. Trend Micro. Available at: https://documents.trendmicro.com/assets/wp/wp-prototype-nation.pdf

Hyslip, T. S. (2020). Cybercrime-as-a-Service Operations. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 815-846. doi: 10.1007/978-3-319-78440-3_36.

Hyslip, T. S., & Holt, T. J. (2019). Assessing the capacity of DRDoS-for-hire services in cybercrime markets. *Deviant Behavior*, 40(12), 1609-1625. doi: 10.1080/01639625.2019.1616489.

Jianwei, Zhuge & Lion, Gu & Duan, Haixin & Roberts, Taylor. (2015). Investigating the Chinese Online Underground Economy. 10.1093/acprof:oso/9780190201265.003.0004.

Koivula, E. M. (2021). Investigation into cybercrime trends. https://www.theseus.fi/bitstream/handle/10024/505576/Koivula_Elias.pdf

Lewis, J. (2018). *Economic Impact of Cybercrime—No Slowing Down Report*. McAfee. Available at: https://assets.website-files.com/5bd672d1924b9893a632c807/5c171d5e85ed62697a79e351_economic-impact-cybercrime.pdf

Lusthaus, J. (2018a). Honour Among (Cyber)thieves? *European Journal of Sociology, 59*(2), 191-223. doi:10.1017/S0003975618000115

Lusthaus, J. (2018b). *Industry of Anonymity: Inside the Business of Cybercrime*. Harvard University Press.

Lusthaus, J. & Varese, F. (2017). Offline and Local: The Hidden Face of Cybercrime. *Policing: A Journal of Policy and Practice, 15*(1) 2021, 4–14. doi: https://doi.org/10.1093/police/pax042

Manky, D. (2013). Cybercrime as a service: a very modern business. *Computer Fraud & Security*, 2013(6), 9-13. oi: 10.1016/S1361-3723(13)70053-8.

Mercês, F. (2014). *The Brazilian Underground Market: The Market for Cybercriminal Wannabes?*. Trend Micro. Available at: https://documents.trendmicro.com/assets/wp/wp-the-brazilian-underground-market.pdf

Trend Micro (2015a). *Ascending the Ranks: The Brazilian Cybercriminal Underground in 2015*. Trend Micro. Available at: https://documents.trendmicro.com/assets/wp/wp-ascending-the-ranks.pdf

Trend Micro (2015b). *German U-Markt: Carving a Niche in the Global Black Market*. Trend Micro. Available at: https://documents.trendmicro.com/assets/wp/wp-u-markt.pdf

Trend Micro (2016a). *Cybercrime and the Deep Web*. Available at: https://documents.trendmicro.com/assets/wp/wp-cybercrime-and-the-deep-web.pdf

Trend Micro (2016b). *Espionage as a Service: A Means to Instigate Economic Espionage*. Available at: https://documents.trendmicro.com/images/TEx/guides/exec-brief-espionage-as-a-service.pdf

Trend Micro (2019). *The Rise of Physical Crime in the Cybercrime Underground*. Available at: https://www.trendmicro.com/vinfo/in/security/news/cybercrime-and-digital-threats/the-rise-of-physical-crime-in-the-cybercrime-underground

Trend Micro (2020). *LokiBot Impersonates Popular Game Launcher*. Available at: https://www.trendmicro.com/en_us/research/20/b/lokibot-impersonates-popular-game-launcher-and-drops-compiled-c-code-file.html

Urano, A. (2015). *The Japanese Underground*. Trend Micro. Available at: https://documents.trendmicro.com/assets/wp/wp-the-japanese-underground.pdf

Wainwright, R., & Cilluffo, F. J. (2017). *Responding to Cybercrime at Scale: Operation Avalanche—A Case Study*. Center for Cyber and Homeland Security at Auburn University.

Wilhoit, K. and Hilt, S. (2015). *North American Underground: The Glass Market*, Trend Micro. Available at: https://documents.trendmicro.com/assets/wp/wp-north-american-underground.pdf

The information, documentation and figures available in this deliverable were produced by the CC-DRIVER consortium under EC grant agreement No. 883543. The views expressed in this document should in no way be taken to reflect the views of the European Commission, nor can the European Commission be liable for any use made of the information contained herein. The commercial use of any information contained in this document may require a licence from the proprietor of that information. Neither the CC-DRIVER consortium as a whole nor any partner in the CC-DRIVER consortium warrant that the information contained in this document is capable of use, nor that use of the information is free from risk, nor do they accept any liability for loss or damage suffered from using this information

This project has received funding from the European Union's Horizon 2020 research and innovation program under grant agreement No 883543.