CC-DRIVER

Understanding the drivers of cybercriminality, and new methods to prevent, investigate and mitigate cybercriminal behaviour.
A Research – CC-DRIVER

D2.2 – Drivers, Trends, and Technology Evolution in Cybercrime

[WP2 – Scoping cybercriminality and technical capabilities]

Lead contributor	Evangelos Markatos, FORTH
Other contributors	Mary Aiken, UEL
	Rubén Fernández Bleda, PLV
	Otilia Bularca, SIMAVI
	Afonso César, PJ
	Julia Davidson, UEL
	Lavinia Dinca, SIMAVI
	Lucas Echard, FSC
	Ruby Farr, UEL
	Sven-Eric Fikenscher, BayHfoeD
	Anton Keskisaari, FSC

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

Alexey Kirichenko, FSC
Elias Koivula, FSC
Antonis Krithinakis, FORTH
Mohammad Kazem Hassan Nejad, FSC
Willem van der Schoot, FSC
Sini Olkanen, FSC
Maria Patricia Revilla Dacuno, FSC
Kirsty Philips, UEL
Sami Ruohonen, FSC
Amit Tambe, FSC
Johannes Töyli, FSC
Anthony Joe Melgarejo, FSC
David Wright, TRI

Due date	31.10.2021
Delivery date	31.10.2021 (updated version 6.03.2021)
Type	Report
Dissemination level	PU = Public This deliverable has been reviewed by the CC-DRIVER Security Advisory Board (SAB) who concur with the existing classification of the deliverable. The SAB comprises the following members: Dr Philipp Amann of Europol's European Cyber Crime Centre; Dr Holger Nitsch of Hochschule für den öffentlichen Dienst in Bayern (Bavarian police academy) [BayHfoeD], José Luis Diego of Valencia Local Police [PLV] and Lúcia Lebre of Directorate-General Innovation and Development, Polícia Judiciária.

Keywords	cybercrime, technical drivers, human drivers

1. Abstract

In this report, (i) we identify and analyse the technical and human drivers of cybercriminality and (ii) we review techniques and tactics of cybercriminals and cybercrime-as-a-service. On the technical side, we investigate the developments that facilitate criminality, the availability of hacking tools online, cryptocurrencies, and the widespread use of anonymity and the Dark Web. On the human side, the focus is on drivers that enable and/or allow humans to act differently online. In particular, human behaviour may be influenced by such factors as anonymity, disinhibition, minimisation of status and authority, along with normalisation and socialisation in technology-mediated environments. With respect to the techniques and tactics of cybercriminals, we review tools, vulnerabilities and emerging attacks. We pay special attention to cybercrime-as-a-service and its technical and illegal business aspects, including a study of the evolution of websites that support cybercriminal services over time.
We explore the connections between cybercrime and crime in the physical world, including hybrid forms of crime as well as traditional crime enabled by cyber activities (such as advanced cyber intelligence used for criminal purposes).

Revision Procedure

Version	Date	Description	Reason for Change	Author(s)
2.0	1.05.2021	First draft	-	
3.0	16.08.2021	First complete draft		
4.0	27.07.2021	Copy-edited version		
5.0	07/10/2021	Reviewed version		
6.0	15/10/2021	Addressed reviewer comments		
7.0	27/10/2021	Addressed SAB comments		
8.0	24/12/2021	New version to address EC review comments		
9.0	9/1/2022	Addressed review comments		
10.0	4/3/2022	Final version for re-submission		

Contents

1. ABSTRACT ... 3
2. EXECUTIVE SUMMARY ... 7
3. LIST OF FIGURES ... 9
4. LIST OF TABLES ... 10
5. LIST OF ACRONYMS/ABBREVIATIONS ... 11
6. KEY TERMINOLOGY AND WORKING DEFINITIONS ... 16
1 INTRODUCTION ... 19
1.1 BACKGROUND ... 19
1.2 OBJECTIVES ... 19
1.3 STRUCTURE OF THE REPORT ... 20
1.4 DEFINITIONS ... 20
1.5 SCOPE AND LIMITATIONS ... 23
1.6 INDEX OF CYBERCRIMES COVERED IN THIS REPORT ... 26
2 METHODOLOGY ... 27
3 TECHNICAL DRIVERS OF CYBERCRIME ... 29
3.1 AVAILABILITY OF HACKING TOOLS ON THE INTERNET ... 31
3.2 CYBER VULNERABILITIES ... 32
3.3 MARKETPLACES ... 34
3.4 MESSAGING APPS ... 35
3.5 ANONYMISING SERVICES, THE TOR NETWORK AND DARK WEB ... 37
3.6 DEEP WEB ... 38
3.7 HOSTING SERVICES ... 39
3.8 CRYPTOCURRENCIES ... 40
3.9 AVAILABILITY OF CRYPTOGRAPHY TECHNIQUES ... 41
3.10 IOT AND CPS ... 41
3.11 SUPPLY CHAINS ... 43
3.12 CLOUD PLATFORMS ... 44
3.13 SOCIAL MEDIA ... 45
4 HUMAN DRIVERS OF CYBERCRIME ... 51
4.1 APPROACH AND METHODOLOGY ... 52
4.2 INTRODUCTION ... 54
4.3 MULTIDISCIPLINARY APPROACH TO UNDERSTANDING CYBERCRIME ... 60
4.4 PROFILING CYBERCRIMINAL OFFENDERS FROM TYPES OF CYBERCRIME ACTS ... 68
4.5 CONCLUSION ... 92
5 TECHNIQUES, TACTICS AND TOOLS OF CYBERCRIMINALS ... 94
5.1 HACKING AND DUAL-USE TOOLS ... 98
5.2 MALWARE ... 103
5.3 EXPLOITATION ... 144
5.4 EMERGING ATTACKS ON IOT AND CPS ... 154
5.5 USE OF WEBSITES AND HOSTING SERVICES ... 155
5.6 SOCIAL ENGINEERING, USE OF 'HUMAN' VULNERABILITIES ... 157
5.7 SUPPLY CHAIN ATTACKS ... 160
5.8 ATTACKS ON CLOUD PLATFORMS ... 168
5.9 ATTACKS ON COLLABORATION PLATFORMS AND TOOLS ... 170
5.10 CYBERSTALKING ... 172
5.11 IDENTITY THEFT - THEFT OF BANK CARDS ... 174
5.12 DRUG CRIME ... 175
5.13 HUMAN TRAFFICKING ... 177
5.14 CSAM ... 178
5.15 ONLINE HARASSMENT - CYBERBULLYING ... 180

5.16 EXTORTION – SEXTORTION 181
5.17 GROOMING 182
5.18 REVENGE PORN 183
5.19 HATE SPEECH 184
5.20 CYBER TERRORISM – VIOLENT EXTREMISM - RADICALISATION 185
5.21 THE GENDER DIMENSION 186
5.22 THE GEOGRAPHICAL DIMENSION OF CYBERCRIME 189
5.23 THE AGE DIMENSION OF CYBERCRIME 197
6 CYBERCRIME-AS-A-SERVICE (CAAS) 199
6.1 CRYPTOCURRENCY LAUNDERING AND TUMBLING 201
6.2 BULLETPROOF HOSTING 202
6.3 TUTORIALS, TRAINING AND CONSULTING 204
6.4 HACKING-AS-A-SERVICE 204
6.5 CODING/PROGRAMMING-AS-A-SERVICE 205
6.6 CRYPTING - OBFUSCATION 205
6.7 DISTRIBUTED DENIAL-OF-SERVICE (DDOS) ATTACKS/REFLECTION ATTACKS (DRDOS) 206
6.8 SMS FLOODING AND SPAMMING 209
6.9 ESCROW/GARANT/TREUHAND 209
6.10 FAST-FLUXING - A MOVING TARGET 210
6.11 MULES 212
6.12 PROXY SERVERS 213
6.13 VPN SERVERS 214
6.14 EMAIL SPAMMING AND PHISHING 214
6.15 CRIMEWARE - RANSOMWARE-AS-A-SERVICE 215
6.16 DATA-AS-A-SERVICE (DAAS) 217
6.17 SERIAL KEYS - PIRATED SOFTWARE 220
6.18 SOCIAL BOOSTERS - FRIENDS AND "LIKES" FOR PURCHASE 221
6.19 WEB TRAFFIC - VISITORS 221
6.20 CYBERCRIMINAL BUSINESS, MARKETING AND MESSAGING 222
6.21 UNDERGROUND FORUM ACCESS 223
7 CONNECTIONS BETWEEN CYBER AND TRADITIONAL CRIME 226
8 TRENDS AND CORRELATIONS IN THE CYBERCRIME LANDSCAPE 229
8.1 SERVICE MODELS 229
8.2 MALWARE 230
8.3 COMMUNICATION METHODS 234
8.4 MONETISATION 237
8.5 SUMMARY 242
9 LEA INVOLVEMENT IN COUNTERING CYBERCRIME AND DEALING WITH ITS DRIVERS 244
10 CONCLUSION 249
11 REFERENCES 250

2. Executive summary

This document identifies the main technical and human drivers of cybercrime.

Technical drivers of cybercrime include:

- **Vulnerabilities:** Software (and, in some cases, the hardware) contains **bugs** that are the result of programming errors. Since software is written by people, and since people make mistakes, such software bugs are unlikely to be completely eradicated in the near future. Cybercriminals use these mistakes (bugs) to trigger vulnerabilities and illegally gain access to remote computers. These bugs are usually the main technical vehicle that cybercriminals use to compromise remote computers and commit a variety of cybercrimes including extortion, blackmailing, spying, stalking, etc.
- **Anonymity**. There exist several tools (apps, VPNs, Dark Web, anonymising networks) that allow cybercriminals to hide their real identity and operate (almost) anonymously. Such anonymity makes it difficult for law enforcement authorities (LEAs) to trace the criminal activities to the human perpetrators. As a result, under the cloak of this anonymity, cybercriminals may perform a wide variety of illegal activities that would not otherwise be possible.
- **Cryptocurrencies**. Over the past few years, we have seen an increase in cryptocurrencies, whose market capitalisation is now valued at more than US$ 1 trillion. Some of these currencies provide pseudonymity or even complete anonymity. Such currencies, which for the most part are not regulated, enable cybercriminals to send and receive money (almost) anonymously, facilitating crimes including money laundering, extortion, drug sales, trafficking, etc.
- **Cybercrime-as-a-service**. Over the past years, we have seen entities offering cybercrime services (e.g., DoS attacks, hacking tools, botnets for hire, etc.) and products (e.g., malware) "as-a-service" to aspiring cyber criminals who do not have the technical skills to develop such products or services themselves. This implies that the number of cybercriminals may increase significantly, as they can purchase (almost) all the tools they need in order to engage in cybercrime.
- **An expanding attack surface**. Over the past few years, an increasing number of devices are being equipped with computing and communication capabilities. We all hear about smart cars, smart TVs, smart light bulbs, smart fridges, smart coffee makers, etc. This "smart" adjective essentially means that these devices can now connect to the Internet and have some (basic) computational capabilities. As a result, the number of computing devices that are connected to the Internet is increasing, and so is the number of potential targets for cybercriminals.[1]
- **Computers interacting with the physical world**. Internet-connected computers are increasingly used to control traditional infrastructures: energy grids, water supplies, and medical equipment are all controlled by computers connected (directly or indirectly) to

[1] This was clearly articulated to a large extent in the call for proposals which stated: "The Internet of Things, the ever increasing number of internet-connected devices, may pose substantial threats to (cyber)security since this fully connected world as well as the network itself have become a target for cybercriminals."

> the Internet. This interaction with the physical world makes those computers attractive targets for cybercrime. Attacking such computers may have a devastating impact on people's lives: blackouts in the middle of the winter, hospitals unable to provide health care, energy companies unable to provide gas to their customers.

On the human driver side, we explore key theories from four academic disciplines, namely, criminology (including cybercriminology), psychology, cyberpsychology and neuroscience, and question what they might tell us about human drivers of cybercrime. We argue that a multidisciplinary approach is the key to a holistic understanding of the human drivers behind cybercriminal action and intent. We discuss the potential motives and drivers behind the tactics, techniques and procedures (TTPs) of five different cyber-dependent cybercriminal acts—namely, hacking, malware writing, use of ransomware, use of remote access trojans (RATs) and engagement in cybercriminal networks—drawing linkages throughout between cyber-dependent crime, traditional crimes, cyber-enabled crime and deviant behaviours. We recognise the vast complexities that must be factored in when considering human behaviour, the multi-faceted nature of human drivers of cybercrime and cyber delinquency, arguably compounded by the tendency for people to behave differently in cyberspace than in real-world contexts. We also explore the cybercrime trends experienced worldwide during the Covid-19 pandemic and discuss related human drivers at play.

3. List of figures

Figure 1: A Word cloud of the more than 250 references in our bibliography. 28
Figure 2: The architecture of the tor anonymity network. 38
Figure 3: Regional cybercrime trends during the pandemic (INTERPOL, 2020, p6-7) visualised by UEL on a global map 59
Figure 4: Taking a multidisciplinary approach 60
Figure 5: Block's proposed excessive use framework presented visually by UEL 67
Figure 6: Malware process 'components' summary (Kirwan G. & Power 2012., The Psychology of Cyber Crime: Concepts and Principles, pp. 78-79). 77
Figure 7: Blackhole exploit kit advertising pricing for access and rent to exploit kit. 130
Figure 8: Neutrino exploit kit prI would also work the Monday after my holiday rather than having that day off to catch up that week as best as possible. icing 2013 134
Figure 9: Neutrino exploit kit pricing 2014 135
Figure 10:Nuclear exploit kit pricing 136
Figure 11: Percentage of convicted offenders for Human Trafficking. We see that in overall (Global – first bar) 64% are male and 36% are female. Source: UNODC, Global Report on Trafficking in Persons 2020 (United Nations publication, Sales No. E.20.IV.3). 188
Figure 12: Map of Cybercrime. The map shows the "number of European States which have identified criminal suspects and/or infrastructure" in each country. Darker colors mean that more European States have identified criminal suspects in this country. We see that the countries that top the list are Nigeria, China USA, and Germany. Significant roles are also played by Russia, Canada, India, Australia, Brazil, etc. Source: Europol https://www.europol.europa.eu/iocta/2016/resources/iocta-2016.pdf 189
Figure 13: Offerings for "Cybercrime-as-a-Service". Aspiring cybercriminals may purchase these offerings on-line and thus ease their way into conducting cybercriminal activities. 200
Figure 14:Insurance claims of cyber incidents (Coalition, 2020) 231
Figure 15: Number of unique ransomware families/variants (F-SECURE, 2018). 232
Figure 16: Number of detection reports per year based on percentage of total # of ransomware detections from 2015-2017 (F-SECURE, 2018) 232
Figure 17: Amount of median & average ransom payments by quarter in USD (Coverware) 233
Figure 18: Numbers and growth of new Powershell malware in 2019 and 2021 as observed by McAfee 234
Figure 19: Number of tor relays & bridges since 2008 235
Figure 20: General Telegram popularity has been in a steady growth 237
Figure 21: Bitcoin daily transactions 30 day average (Blockchain.com) 240
Figure 22: Illicit crypto transfers (chainanalysis) 241
Figure 23: Illicit cryptocurrency transfer destinations by type. (chainanalysis) 242

4. List of tables

Table 1: List of acronyms/abbreviations 11
Table 2: Table of Key terminology, working definitions and sources 16
Table 3: Organisational definitions of cybercrime as collated by authors Akdemir, Sungur, and Başaranel (2020). 22
Table 4: Cybercrime motives (Neufeld, 2010) 55
Table 5: Definitions of different types of hackers (from Sabillon et al., 2016, pp. 2-3) 73
Table 6: Forums and forum information in the Crime BB dataset. Source: Akyazi et al. (2021, p. 4) 88

5. List of acronyms/abbreviations

Table 1: 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
IOCTA	Internet Organised Crime Threat Assessment

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

6. Key terminology and working definitions

Table 2: Table of Key terminology, working definitions and sources

Term	Working Definitions	References or Key Texts
Bug	A human mistake in the programming of a computer that makes the computer behave in an erroneous way. Attackers use such bugs to gain unauthorized access to the computer.	See section 3.2.
Cybercrime	For the purposes of the CC-Driver research project the term 'cybercrime' refers to broad spectrum of behaviours encompassing all online behaviours that result in harm; including online harms, cyberdeviance, cyberdelinquency and crimes conducted in cyberspace or through the use of digital technology (Phillips, et al., 2021). This is represented within the new framework presented in D3.1 ("Report on Drivers of Cyber Juvenile Delinquency") on page 20. For a further discussion of cybercrime definitions see Chapter 3 of D2.1 (pp. 15-29) and Chapter 1 of D3.1 (pp.11-20) for a broader discussion of these issues.	See chapter 3 of D2.1, chapter 3 of D3.1 and Phillips et al. (2022).
Cybercrime-as-a-Service (CaaS)	The provision of cybercrime activities "packaged" as services.	See Hyslip, T. S. (2020)
Cybersecurity	"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following: • Availability • Integrity, which may include authenticity and non-repudiation • Confidentiality"	Quote from ITU (ITU, 2009, pp. 2-3)

Cyber-enabled crimes	Cyber-enabled crimes are traditional crimes that predate the advent of the technology, that are now facilitated or have been made easier (i.e., enabled) by cyber technology	Original Source: Brenner (2007)
Cyber-dependent crimes	Cyber-dependent crimes are crimes that arose with the advent of technology and cannot exist (i.e., dependent) outside of the digital world	Original Source: Brenner (2007)
Extortion (Cyber or Online)	Extortion is the act of obtaining money or property by threat to a victim's property or loved ones, intimidation, or false claim of a right (such as pretending to be an IRS agent).	See section 5.16
Hack, Hackers and Hacking	Hacker is a person who illegally gains access to and sometimes tampers with information in a computer system	Merriam Webster dictionary https://www.merriam-webster.com/dictionary/hacker
Human Drivers	The human factors are termed as the individual characteristics of offenders, including the social and psychological processes that play a role in the development of offending. These factors including their online activity play a critical role in forming a person's pathway.	Informed by Leukfeldt (2017) and (Akdemir & Lawless, 2020)
Malware	Software designed to make a malicious action	See section 5.
Markets (Dark Web)	Online marketplaces that are difficult to be traced	See sections 4.4.5.3, 6.20.
Motivations	The motivators are regarded as the "intentions of digital culprits" to commit online misconduct that have led to them to commit or escalate their cyber-related misbehaviour.	Informed by Li (2017), Maiwald (2003) and Jordan and Taylor (1998)
Pathways	The pathways for young people are considered the trajectories of cyber misconduct which instigates their involvement and how a juvenile is drawn into an illegal/deviant online activity.	Informed by Aiken, Davidson and Amann (2016) and National Cyber Crime Unit / Prevent Team (2017)

Phishing	Phishing – an attempt to trick users through email, social media, etc. into revealing personal information such as passwords.	See section 5.6.
Piracy (Digital or Online)	The un-authorised use of copyrighted material (such as movies, songs, books, software, etc.)	See section 6.17
Ransomware	Malware that blackmails the users of a computer. Ransomware may encrypt the files of a computer and ask for money in order to provide the decryption key. Malware may also discover personal information and threaten the users of the computer of releasing this personal information on the public domain.	See sections 4.4.3, 5.2.2.6.
Remote Access Trojan (RAT)	RAT is a type of malware that allows an attacker to control a system from a remote location.	See section 5.2.2.2.
Surface web	The portion of the World Wide Web that is available to all. Surface web is composed of all web sites accessed by search engines. On the contrary, Deep web is the portion of the World Wide Web that needs special privileges (e.g. a password) to be accessed.	See section 3.6.
Technical Drivers	Technical Drives of cybercrime are the technological developments that made cybercrime easier.	See section 3.
Virus	A piece of code that attaches itself to a computer program and usually performs some malicious operation	See sections 4.4.2.1, 5.2.1.

1 Introduction

1.1 BACKGROUND 19
1.2 OBJECTIVES 19
1.3 STRUCTURE OF THE REPORT 20
1.4 DEFINITIONS 20
1.4.1 Cybercrime 20
1.4.2 Cybercrime not "cybersecurity" 21
1.5 SCOPE AND LIMITATIONS 23
1.6 INDEX OF CYBERCRIMES COVERED IN THIS REPORT 26

1.1 Background

This report is being drawn up in the context of the CC-DRIVER project (https://www.ccdriver-h2020.com/) funded by the European Commission. CC-DRIVER aims to investigate, identify and explain drivers of new forms of cybercriminality. It specifically focuses on understanding human factors that determine criminal behaviours, online disinhibition and young people's decision-making processes. Thus, in a collective effort to combat cybercrime, CC-DRIVER improves our understanding of the technical and human factors that determine cybercriminal behaviours, especially in young people. To that end, CC-DRIVER uses a multidisciplinary approach and includes the following scientific domains: (i) psychology, (ii) criminology, (iii) anthropology, (iv) neurobiology and (v) cyberpsychology. The report draws on the work done in deliverables D2.1 and D3.1 (with respect to the fundamentals and definitions of cybercrime) but goes well beyond these deliverables with respect to the exploration of the drivers of cybercrime. The results of these documents are fed to the subsequent WorkPackages of the project including WP5 and WP7.

1.2 Objectives

The overarching objective of this report is to improve our understanding of cybercrime through (i) the description of the technical drivers that make cybercrime easier and (ii) the description of the human drivers that push (mostly young) people to cybercrime—possibly people who would not otherwise engage in more traditional (i.e., non-cyber) forms of crime. Specific questions that we would like to answer include:

- Which technical developments make cybercrime easier and more effective?
- Which technical developments increase the opportunities for cybercrime?
- Which human factors drive people (especially the young ones) into cybercrime?

1.3 Structure of the report

This report has nine sections and approaches topics ranging from the drivers (technical and human aspects) of cybercrime to the tools and services deployed by cybercriminals, to the cybercrime landscape (traditional and cybercrime connections) and the measures employed by LEAs to fight against cybercriminality. The sections are summarised as follows:

- **Section 2** presents the methodology used in the research.
- **Section 3** focuses on the technical drivers of cybercrime, that is, the technologies that make cybercrime easier (or even possible).
- **Section 4** focuses on the human aspects of cybercrime, that is, what drives humans to get involved in cybercrime particularly (as opposed to other kinds of more traditional crime).
- **Section 5** describes the techniques, tactics and tools used by cybercriminals. Such tools may involve hacking tools, malware, etc.
- **Section 6** describes cybercrime-as-a-service. Indeed, cybercrime has become so complicated and consists of so many components, that some of these components are now offered as a service. Such components may involve anonymising networks, malware kits, anonymous payments, etc.
- **Section 7** explores the connections between cybercrime and traditional crime.
- **Section 8** describes trends and correlations in the cybercrime landscape.
- **Section 9** describes the involvement of LEAs in countering cybercrime.
- **Section 10** concludes the report.

1.4 Definitions

1.4.1 Cybercrime

Defining crime related phenomena hinges on two different yet related factors: "*the behavior as behavior, and … the definitions by which specific behavior comes to be considered crime or non-crime*" (Vold, 1958, p. vi), and there is almost always some tension due to this fact. Having a clear conceptualisation is key, as even small variations in the conceptualisation of cybercrime could affect the measurement of, and response to, cybercrime behaviours (McGuire, 2020).

The only well recognised consensus within academic literature is that there is no single, clear, and broadly accepted definition of cybercrime (Phillips, et al., 2021). According to a recent review (Akdemir, Sungur, & Başaranel, 2020) the two most commonly cited definitions in academia are: "*computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks*" (Thomas & Loader, 2000, p. 3); and, "*any crime that is facilitated or committed using a computer, network, or hardware device*" (Gordon & Ford, 2006, p. 14).

A cybercrime distinction originally proposed by Brenner (2007) is the most widely used categorisation system consistently adopted by researchers and policy makers (e.g., see McGuire and Dowling, 2013):

- ***Cyber-dependent crimes** are crimes that arose with the advent of technology and cannot exist (i.e., dependent) outside of the digital world*
- ***Cyber-enabled crimes** are traditional crimes that predate the advent of the technology, that are now facilitated or have been made easier (i.e., enabled) by cyber technology*

Problematically however both these definitions are still rooted in what is a crime or what is considered illegal. This fundamentally creates confusion and variation in what is meant by 'cybercrime' as legal statues vary across jurisdictions, there is no consistent interpretation as to what offences are considered in scope and this is further compounded by the fact that typically cybercriminal behaviours outpace the introduction of legal statutes (Phillips, et al., 2021). All of these factors and inconsistencies in conceptualisation of cybercrime hamper the measurement and understanding of cybercrime across jurisdictions and across disciplines, the legal responses to cybercrime and global initiatives and cooperative efforts to tackle cybercrime. The key definitions identified here are however indicative of a broad range of behaviours, and this is appropriately representative of the broad range of behaviours that are encompassed under the umbrella term of 'cybercrime'.

Therefore, for the purposes of the CC-DRIVER research project the term 'cybercrime' refers to a broad spectrum of behaviours encompassing all online behaviours that result in harm ; including online harms, cyberdeviance, cyberdelinquency and crimes (both cyber-dependent and cyber-enabled) conducted in cyberspace or through the use of digital technology (Phillips, et al., 2021). This is represented within the new framework presented in D3.1 ("Report on Drivers of Cyber Juvenile Delinquency") on page 20. For a further discussion of cybercrime definitions see Chapter 3 of D2.1 (pp. 15-29) and Chapter 1 of D3.1 (pp.11-20) for a broader discussion of these issues.

1.4.2 Cybercrime not "cybersecurity"

Cybersecurity definitions are as diverse and ambiguous as cybercrime definitions (e.g. see reviews conducted by Craigen, Diakun-Thibault and Purse, 2014, and ENISA, 2015). However, as shown in the definition below provided by the ITU (2009, pp. 2-3), cybersecurity mainly concerns protection of technological assets and protection from cybercriminal attacks against availability, integrity and confidentiality of computer data and systems. This wording corresponds to category 1 offenses in The Council of Europe's Convention of Cybercrime (2001) typology ("Offenses against the confidentiality, integrity, and availability of computer data and systems").

> *"Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:*
>
> *Availability*
>
> *Integrity, which may include authenticity and non-repudiation*
>
> *Confidentiality"*
>
> Source: (ITU, 2009, pp. 2-3)

A consistent problem in certain domains is that the term 'cybercrime' is often used to refer to cybersecurity-based offenses only, meaning there is disproportionate focus on more technical, cyber-dependent or category 1 type offenses, this is demonstrable in organisational definitions of cybercrime currently in use by key European and international organisations - shown in Table 3. Therefore, narrow definitions of cybercrime (only considering technical crimes) are perhaps more aptly described as representative of 'cybersecurity' offenses (narrow) rather than 'cybercrime' (broad). CC-DRIVER's definition of cybercrime encompasses a broad range of behaviours, with equal focus on both cyber-dependent and cyber-enabled offenses.

Table 3: Organisational definitions of cybercrime as collated by authors Akdemir, Sungur, and Başaranel (2020).

Year	Organisation	Definition of cybercrime
1994	The United Nations	"The United Nations manual (United Nations, 1994) on the prevention and control of computer-related crime (1994) uses the terms, computer crime and computer-related crime interchangeably. This manual did not provide any definition" (Akdemir, Sungur, & Başaranel, 2020, p. 116)
2000	The Tenth United Nations Congress on the Prevention of Crime and the Treatment of Offenders	1. "any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them." 2. "any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network" (UN Congress, 2000, p. 5)
2001	The Council of Europe Cybercrime Convention (a.k.a. The Budapest Convention)	"action directed against the confidentiality, integrity and availability of computer systems, networks and computer data as well as the misuse of such systems, networks and data by providing for the criminalisation of such conduct" (Council of Europe , 2001, p. 2)
2007	The Commission of European Communities	"criminal acts committed using electronic communications networks and information systems or against such networks and systems" (Commission of the European Communities, 2007, p. 2)
2013	Shanghai Cooperation Organization (SCO) Agreement	"the use of information resources and (or) the impact on them in the informational sphere for illegal purposes" (cited in Malby et al. (2013, p. 15))

2013	Cybersecurity Strategy of the European Union	"a broad range of different criminal activities where computers and information systems are involved either as a primary tool or as a primary target" (European Commission, 2013, p. 3)
2016	Commonwealth of Independent States Agreement	"a criminal act of which the target is computer information" (cited in Akhgar et al., 2016)

In this deliverable, although we cover most of the areas of cybercrime, we particularly focus in cyber-dependent crime[2] (i) as this is the main focus area of the European Cybercrime Centre or Europol[3], and (ii) as this seems to be the thrust of the call for proposals which observes "*a rise in adolescent hacking*" and calls for "*providing alternatives to harness the potential of these young talents for cybersecurity and technologies*"[4]

1.5 Scope and limitations

Cybercrime is defined above in the glossary of terms on page 16 as; a broad spectrum of behaviours encompassing all online behaviours that result in harm; including online harms, cyberdeviance, cyberdelinquency and crimes conducted in cyberspace or through the use of digital technology (Phillips, et al., 2022). For a further discussion of cybercrime definitions and broader discussion on definitional issues, see Chapter 3 of D2.1 (pp. 15-29) and Chapter 1 of D3.1 (pp.11-20).

Key to conceptualising cybercrime is the distinction between cyber-dependent and cyber-enabled crimes (also defined above in the glossary of terms) (Brenner, 2007). Cyber-dependent crimes are crimes that arose with the advent of technology and cannot exist (i.e., dependent) outside of the digital world, whereas cyber-enabled crimes are traditional crimes that predate the advent of the technology, that are now facilitated or have been made easier (i.e., enabled) by cyber technology. This distinction in how cybercrime is conceptualized is widely used and consistently adopted by researchers and policy makers (McGuire & Dowling, 2013; Sarre, Lau, & Chang, 2018; Paoli, Visschers, Verstraete, & Van Hellemont, 2018).

The purpose of T2.2/D2.2., according to the Grant Agreement, is to analyse drivers of *new* forms of cybercriminality. The secondary purpose of T2.2/D2.2, according to the Grant Agreement, is to contribute to Result 1: a landscape study of 'Cybercrime-as-a-Service' (CaaS). To fulfil this specification this report primarily focuses on cyber-dependent cybercrimes. The Council of Europe's (COE) Convention of Cybercrime (2001) is the "*the only globally recognized agreement around cybercrime*" (McGuire M. , 2020, p. 19) and this framework groups cyber-dependent cybercrimes as 'Category 1: Offences against the confidentiality, integrity and availability of computer data and systems', namely: Illegal access; Illegal interception; Data interference; System interference; and, Misuse of devices. This wording is

[2] EC3 differentiates "payment fraud" from "cyber-dependent" crime. Some other definitions put (cyber/computer)-fraud under cyberdepedent crime (see D3.1).
[3] The third focus of EC3 is CSAM covered in section 0. See also https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
[4] https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-fct01-2018-2019-2020

adopted in cybercrime legislation and may encompass a number of cybercriminal behaviours which are explored within this report, namely; hacking, use of malware, use of viruses, cybercrime-as-a-service operations, and trade via cybercrime markets, see the index in 1.5 for where these behaviours are covered within this report.

Whilst the purpose of this report necessitates a focus on cyber-dependent crimes, CC-Driver acknowledges there is a consistent problem in that certain domains use the term 'cybercrime' to refer to cyber-dependent or category 1 type offenses only, meaning there is disproportionate focus on these newer and more technical types of cybercrime (Phillips, et al., 2022). Therefore, this report has sought, where literature is available, to identify newly evolving manifestations of cyber-enabled crimes in digital contexts. These manifestations may encompass either entirely novel forms of criminal behaviours when online (i.e., the creation of unique criminal behaviours in digital contexts), the criminal behaviour itself presents differently in digital contexts compared to real world contexts, or are widely proliferated by the use of digital tools and the affordances of the digital environment (e.g. ways to enhance anonymity). These manifestations of cyber-enabled crimes have been explored in relation to four key areas, as shown below:

Groupings from D3.1	Behaviours that pre-date technology:	Unique manifestations in digital contexts:
Attacks against property or theft	Fraud, forgery and identity theft	Spam, Phishing, Cat fishing
Interpersonal Violence	Harassment, Extortion	Trolling, Cyberbulling, extortion in the form of Romance Fraud
Sexual Violence	CSAM, Grooming, Image based abuse	CSAM Markets, Online Grooming, Revenge Porn (often accompanied with doxxing), Sextortion
Organised crime	Sale of illegal items, money laundering	Dark web markets, money muling

Therefore, these forms of criminality that manifest uniquely in the online environment are brought within scope of this report; and a secondary aim of this report will be to explore the evolving and unique manifestations of cyber-enabled crimes identified above, see section 1.5 (below) for an index of where these behaviours are covered within this report. Cybercrime is an ever-evolving phenomenon, and whilst some features of the crime may stay the same (for example the aim of a cybercriminal act or crime being committed, e.g., illegal access, interference or interception) there can be significant differences in modus operandi that is, tactics, techniques and procedures of cybercriminals. Furthermore, the introduction of new technologies (e.g., a zero-day vulnerability, a new malware or introduction of 5G) and new contexts (e.g., IoT, COVID-19 for example see Aiken, Farr and Witschi, 2022, pandemic

lockdowns) creates further criminogenic mediums, attack vectors and opportunities for cybercriminals and cybercrime operations.

The presence of various technical drivers impacts the ways in which cybercrimes are enacted. Thus, within this report, technical drivers are explored in relation to: cyber vulnerabilities; marketplaces; techniques, tactics and tools (including hacking, types of trojan malware and botnets, exploits). The newly developed "Cybercrime-as-a-Service" business model has completely changed the way cybercrime is conducted and has the potential to completely revolutionize the cybercrime landscape. At the same time, the rapid increase of the attack surface through the proliferation of the Internet of Things gives a new generation of aspiring cybercriminals the entry points they need to commit their nefarious activities.

Human drivers, include the intrapersonal, interpersonal and sociological contexts that may motivate or drive an individual to offend and how the propensity to offend may be amplified in digital contexts. In this report, within the scope defined above, human drivers are explored in relation to theories and predictions of key academic theories (including criminology, psychology, cyberpsychology and neuroscience), the profiles of different types of cyber offenders (hackers, malware users and writers, ransomware users and RAT users) and links to other types of crimes, and finally how the presence of offender convergence settings (where cybercriminals converge online to meet, communicate, coordinate, commit cybercrimes and conduct "as-a-Service" operations, see section 4.4.5) may facilitate cybercriminal activities.

The aim of this report, therefore, is to explore the human and technical drivers of these forms of cybercriminality, with a primary focus on behaviours in relation cyber-dependent crimes and a secondary focus on of cyber-enabled crimes

1.6 Index of cybercrimes covered in this report

Cyber-dependent	1. Attacks Against Data and Systems	Hacking	See sections 3.1, 5.1, and 6.4
		Malware	See sections 5.2 and 8.2
		Cyberespionage	See section 4.4.4.2, 5.2.2.2.9, and 5.2.2.5
	2. Attacks Against Property or Theft	Phishing	See sections 5.6 and 6.14
Cyber-enabled		Digital Piracy	See sections 6.17
		Spam	See sections 6.8 and 6.14
		Fraud	See section 3.13.3, 4.4.3.3, 5.2.2.4.5, and 7
		Identity Theft	See section 5.11
	3. Interpersonal Violence	Cyberbullying	See section 5.15
		Extortion	See section 5.16
		Romance Fraud	See sections 3.13.3 and 4.4.3.3
	4. Sexual Violence	OCSEA	See section 4.4.5.3, and 5.14
		Image-based abuse	See section 5.18
		Sextortion	See sections 5.16 and 4.4.3.3
		Sex trafficking	See section 5.13
	5. Violence Against Groups	Terrorism	See section 5.20
	6. Incidental Use	Laundering/Money Muling	See sections 4.4.5.4 and 6.11
	7. Cross-category factors: Organised Crime	Darkweb markets	See section 3.5
		Cybercrime-as-a-Service (CaaS)	See section 6

2 Methodology

To determine the main technical and human drivers of cybercrime, we carried out a literature review. The literature review is the most appropriate method, given that the level of completeness and comprehensiveness can be parametrised by researchers. The synthesis is in the form of a narrative and findings are collated under themes, guided by the research aims and objectives (Grant & Booth, 2009, p. 94).

The primary texts informing this review in the area of human drivers of cybercrime were:

- Gráinne Kirwan, *The Psychology of Cyber Crime: Concepts and Principles*, 2011
- Gráinne Kirwan and Andrew Power, *Cybercrime: the Psychology of Online Offenders*, 2013
- Thomas J. Holt and Adam M. Bossler, *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 2020.
- Jonathan Lusthaus, *Industry of Anonymity*, 2018.

The first and second are foundational texts in the field of cyber forensic profiling and, while these texts are unique, the findings in both will be approximately 8-10 years out of date when the present text is published; therefore, we included the third and fourth texts as a primary resource, as a recently published review that incorporates chapters from various experts in the field. Throughout, we have supplemented sections with targeted searches, using Google Scholar as an academic search engine (for journal articles and academic papers), and Google for grey literature searches, while reputable news outlets were also queried to provide examples. In view of the niche topic of each section, Boolean search strings were devised for each targeted search, relevant to each section in 4.4. Examples of search strings were:

- "dark personality" AND "extortion" AND "cyber"
- "hacking" AND "routine activity theory"
- "spyware" AND "voyeurism" AND "RAT"

In addition to the above books we collected information from several different sources in the literature, totalling more than 250 papers, including:

- Reports from security companies that publish results related to cybersecurity and cybercrime trends. Such companies include F-Secure, Trend Micro, Symantec, etc.
- Reports from EU agencies or organisations that periodically publish results in this area: EUROPOL [e.g., the Internet Organised Crime Threat Assessment (IOCTA) reports], etc.
- Reports from national agencies that publish results about cybercrime, e.g., BKA, (the German Federal Criminal Police Office), etc.
- Reports from International (including non-English) sources

We studied the above material we collected, and we currently report in this document:

- the technical drivers of cybercrime,

- the human drivers of cybercrime,
- the methods and techniques used by cybercriminals,
- the phenomenon of cybercrime-as-a-service
- the connections between cyber and traditional crime
- the trends and correlations in the cybercrime landscape, and finally
- the involvement of LEAs in countering cybercrime and dealing with its drivers.

Figure 1: A Word cloud of the more than 250 references in our bibliography.

3 Technical drivers of cybercrime

3.1 AVAILABILITY OF HACKING TOOLS ON THE INTERNET 31
3.2 CYBER VULNERABILITIES 32
3.2.1 National Vulnerability Database (NVD) 32
3.2.2 OSVDB/VulnDB Open Source Vulnerability Database 33
3.2.3 WhiteSource Vulnerability Database 33
3.2.4 ExploitDB 34
3.3 MARKETPLACES 34
3.3.1 Forums 34
3.3.2 e-shops 35
3.4 MESSAGING APPS 35
3.5 ANONYMISING SERVICES, THE TOR NETWORK AND DARK WEB 37
3.6 DEEP WEB 38
3.7 HOSTING SERVICES 39
3.8 CRYPTOCURRENCIES 40
3.9 AVAILABILITY OF CRYPTOGRAPHY TECHNIQUES 41
3.10 IOT AND CPS 41
3.11 SUPPLY CHAINS 43
3.12 CLOUD PLATFORMS 44
3.13 SOCIAL MEDIA 45
3.13.1 Cyberstalking - sexting 46
3.13.2 Deviant behaviour 47
3.13.3 Scams 48
3.13.4 Victimisation 48
3.13.5 Age and gender 49
3.13.6 Profit: a final note 49

In this section, we identify and analyse the technical developments (i.e technical drivers) that facilitate cybercriminality. Such developments include:

- **Tools** that became available recently and were not (at least, to the same extent) available several years ago. Such tools include anonymising networks (which allow cybercriminals to operate anonymously), cryptocurrencies (which allow cybercriminals to send and receive payments easily and anonymously), bulletproof hosting services (which allow cybercriminals to host their illegal operations for a long time), etc.
- **The increase of cybercrime opportunities.** Over the past few years, many devices have acquired computation and communication capabilities. Indeed, televisions, refrigerators, coffee-makers, light bulbs, cameras, etc., can now be connected to the Internet. All these devices increase the attack surface (i.e., the possible victims for cybercriminals) as they represent potential (and in some cases easy) targets.

In the remainder of this section, we provide a list of modern digital tools, platforms, and services that make it easier for someone to commit a crime in the digital world and monetise the outcome of the illegal activity. We discuss the following categories based on our literature research. For each category and where applicable, we provide examples of cybercrime cases where the corresponding drivers facilitated the whole process:

- Availability of hacking tools on the Internet
- Cyber vulnerabilities
- Marketplaces
- Messaging Apps
- Anonymising services, the Tor network and Dark Web
- Deep web
- Hosting services
- Cryptocurrencies
- Availability of cryptography techniques
- IoT and CPS
- Supply chains
- Cloud platforms, and finally
- Social media

3.1 Availability of hacking tools on the Internet

Cybercriminals usually have technical skills that enable them to compromise remote computers.[5] Although the technical barrier to acquiring such skills used to be high,[6] it has been steadily lowered over time and is now approaching zero, as cybercrime evolves into a *service-based* business model (more in Chapter 6). One factor that has contributed to this end is the online availability of hacking tools and relevant instructions. Standalone tools and detailed instructions on how to use them—or even how to create new ones—are available at little or no cost for the aspiring cyber attacker. This new era of information sharing, where everyone has access to any type of technical recipe, facilitates the involvement of new people, mostly young ones, in cybercrime. Indeed, recent research has demonstrated that more than 61 per cent of hackers get into hacking before they reach the age of 16.[7]

In addition to such tools, which have been specifically designed by cyber criminals to facilitate cybercrime operations, there are many others that could be misused. For example, security researchers and security firms create tools for legitimate purposes, which are later abused by cybercriminals. Take, for example, a tool that scans a network for open ports. This tool can be used by legitimate users who want to find vulnerable computers in order to repair them. However, the same tool can also be abused by cybercriminals who want to find the same vulnerable computers in order to attack them.

Consider, for example, **Cobalt Strike**[8], a tool developed for security researchers that allows them to simulate attacks on customers. Unfortunately, a recent study[9] showed that this tool has also been used for malicious purposes. Indeed, the study showed that Cobalt Strike was used to host more than a quarter of malware command & control servers (C&C) deployed by threat actors. Thus, there is a clear trend: malicious actors use legitimate tools for malicious purposes.

One might think that legal measures could help curb this trend by outlawing the possession of such tools. Indeed, in 2007 and 2008, new cybercrime laws that prohibited the possession, distribution and use of hacking tools took effect in England[10] and Germany[11]. However, there is still a grey zone in the consideration of what *is* a hacking activity and tool. For example, a simple port scan can be considered either legitimate or malicious, depending on the intentions of the actors who perform the scanning. In the US, there is still no federal or state law to explicitly ban port scanning. However, laws similar to those aforementioned could affect the use of security tools that can be used both by ethical security experts to defend their networks and discover vulnerabilities and by black hat hackers to launch attacks.

The availability of hacking tools is also confirmed by recent cease-and-desist visits. Indeed, from late 2013 to early 2017, the UK's National Cyber Crime Unit (NCCU) coordinated more

[5] Note that social engineering may also be used (which does not require technical skills). However, these sections focus mainly on the technical drivers and skills.
[6] Some cybercriminals are excellent programmers able to discover and trigger vulnerabilities commonly known as "zero day" vulnerabilities.
[7] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file
[8] https://www.cobaltstrike.com/
[9] https://www.recordedfuture.com/2020-adversary-infrastructure-report/
[10] https://www.theregister.com/2008/01/02/hacker_toll_ban_guidance/
[11] http://www.beskerming.com/commentary/2007/08/12/249/German_Security_Professionals_in_the_Mist

than 80 cease-and-desist visits where, when applicable, officers gathered extra information about the criminal pathways used by subjects. One of those operations, Operation Dermic, focused on the customers of the Blackshades malware, a tool that provides a variety of malicious features, such as unauthorised remote control and data theft. The results were impressive[12]:

- 60% of the malware customers learned about the malware in hacking forums
- 21% of them found it just by searching the Web
- the remaining 19% stated that they acquired the tool after learning about it from friends.

An important aspect of the same survey is that many subjects entered cybercrime through gaming. After spending a significant amount of time on playing games, and subsequently on modifying and cheating in games, individuals initiate their first interaction with coding, then with hacking, and eventually commit cybercrimes.

3.2 Cyber vulnerabilities

The term "cyber vulnerability" refers to any cyber weakness that can be exploited by a cybercriminal to perform an elevation of privilege (EoP) or an unauthorised operation in general. An alternative definition is that *a vulnerability is generated by a design, implementation or configuration error that can lead to unexpected events where the security of the computer system, network, application, or protocol involved, could be compromised.*[13] Such vulnerabilities tend to be the result of human mistakes, which are usually called "bugs". These mistakes, these bugs, may go undetected for some time until they are discovered by cybercriminals, who use them to compromise computers. One might think that software and hardware developers would make every effort to eradicate such bugs. Indeed, although these developers make every effort to reduce these bugs to a minimum, they have not yet found a way to completely eradicate bugs from all software and hardware that we use: they can reduce them, they can minimise them, but they do not yet know how to completely eradicate them.

Computer systems and protocols have vulnerabilities (bugs) (i) by design, (ii) by mistake and (iii) by lack of good engineering. These vulnerabilities facilitate cybercrime and enable cybercriminals to commit their crimes. In the subsections below, we list some of the most well-known databases of vulnerabilities available today.[14]

3.2.1 National Vulnerability Database (NVD)

The US-based National Vulnerability Database (NVD) is one of the largest databases of known vulnerabilities, in both commercial and open-source frameworks. The NVD includes databases of security checklist references, security-related software flaws, misconfigurations, product names and impact metrics.[15] It is maintained by the NIST Computer Security Division,

[12] https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file
[13]https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/glossary
[14] https://resources.whitesourcesoftware.com/blog-whitesource/open-source-vulnerability-databases
[15] https://nvd.nist.gov/

Information Technology Laboratory, and is sponsored by the Cybersecurity & Infrastructure Security Agency (CISA). NVD builds upon the work of the MITRE Corp. and other organisations and provides information about vulnerabilities and exposures, referred to as Common Vulnerabilities and Exposures (CVE). The CVE system generates an identifier for a given vulnerability, thus making it easier to share information about known vulnerabilities among organisations. This common name is a standard and allows security professionals to access information across multiple sources. As mentioned in the official NVD website, the staff analyse the various CVEs that are published in MITRE's CVE dictionary and generate impact metrics (Common Vulnerability Scoring System, CVSS), vulnerability types (Common Weakness Enumeration, CWE) and applicability statements (Common Platform Enumeration, CPE). In other words, the user can search this database and find information about (i) how a specific vulnerability operates, (ii) what is the vulnerability's impact and (iii) what available workarounds and patches may exist. Moreover, by using the CPE system, a user can find information about vulnerabilities in a specific *version* of an application, a specific operating system or even a specific hardware device.

3.2.2 OSVDB/VulnDB Open Source Vulnerability Database

The Open Source Vulnerability Database (OSVDB) started in August 2002 and was officially launched to the public in March 2004. Using the motto "*Everything is Vulnerable*", the project created a non-commercial database to provide the public with detailed and unbiased technical information on security vulnerabilities. Despite the fact that these data were barred from commercial use without a licence, large companies violated this prohibition[16] without contributing any capital or service back to the community. This uncompensated use of the database led to its permanent closure in 2016. However, by the end of 2011, a new company, Risk-Based Security, had already been created and provided a commercial version of OSVDB, named VulnDB[17]. VulnDB is still active at the time of writing and is available as a paid subscription service.

3.2.3 WhiteSource Vulnerability Database

The WhiteSource Vulnerability Database (WVD) is an open, searchable database that aggregates information from a variety of sources, including the NVD, security advisories and open-source project-issue trackers.[18] For each vulnerability, the database, provides a significant amount of information, including (i) programming language, (ii) the CWE type, (iii) the CVSS impact scores, (iv) verified suggested fixes and (v) help to make informed remediation decisions. The WVD tracks almost a dozen security advisories (such as RubyOnRails, RubySec and Node Security) to include vulnerabilities that may not make it to the CVE/NVD databases. Like security advisories, WVD monitors issue trackers, which are often the first place detected vulnerabilities are reported.

[16] See https://en.wikipedia.org/wiki/Open_Source_Vulnerability_Database
[17] https://vulndb.cyberriskanalytics.com/
[18] https://www.whitesourcesoftware.com/vulnerability-database/

3.2.4 ExploitDB

ExploitDB[19] is a popular database used by penetration testers and vulnerability researchers. It has a free software GPL-2.0 licence and is sponsored by Offensive Security[20]. The database aims to serve as a comprehensive collection of exploits, shellcode and papers. Its most popular use is for providing proofs of concept (PoCs) for vulnerabilities. A proof of concept is a piece of code that demonstrates that a vulnerability exists and that it can be triggered. Security researchers and practitioners use PoCs to demonstrate the existence of a vulnerability and to help towards its removal.

3.3 Marketplaces

Online marketplaces are websites used for selling things online. Typically, a marketplace advertises products and services provided by the website owner or by multiple third parties. The advertisement includes the price and all the information needed by the buyers to determine if the goods are the right fit for them. Many people use online marketplaces to shop without having to visit a physical store. Although marketplaces can be used for legitimate shopping, cybercriminals also use online marketplaces to sell their illegal products and services. Such products include tools that facilitate cybercrime. Aspiring cybercriminals use these tools to facilitate their nefarious activities. Although such marketplaces were initially used mostly to trade credit cards, today they can be used for a wide variety of cybercrime-related products and services. According to recent studies (Benjamin et al., 2015; Du et al., 2018; Hyslip, 2020), cybercriminals create communities and use multiple marketplaces (i) to disseminate knowledge and methodology and (ii) to engage in trading. These marketplaces include forums, e-shops, and IRC channels (see section 3.4). To evade detection and avoid being traced through their IP addresses, several of these marketplaces are active in an anonymous part of the Internet known as the **Dark Web**, an infrastructure analysed in detail in section 3.6.

3.3.1 Forums

Internet forums, also known as message boards, are a specific kind of website where people originate a conversation, post messages and share their thoughts and knowledge on a topic. Forums can be considered as an electronic variation of bulletin boards, used to advertise “items wanted” or “items for sale” and to announce events. Forums usually have a specific tree-like directory structure to organise the topics and to classify visitors and logged-in members into user groups with different privileges and rights.

Underground forums, often described as “hacker” or “hacking” forums, are places where hackers converge to share information (such as cyber intelligence and hacking techniques) and sell cyberattack assets, illegal products and services. In underground forums, one can find a wealth of cybercriminal knowledge in the form of tutorials. Moreover, these forums usually sell products such as hacking tools and malware (see section 5.1) and **cybercrime-as-a-service**

[19] https://www.exploit-db.com/
[20] https://www.offensive-security.com

offerings (Europol, 2014), an emerging trend in the cybercriminal ecosystem, which we discuss in detail in section 6.

VENDORS AND BUYERS IN THE UNDERGROUND FORUM WHO DO NOT TRUST EACH OTHER USE AN **ESCROW** AS A TRUSTED THIRD PARTY TO MITIGATE THEIR TRANSACTIONS.

These forums are well organised and, in several aspects, they resemble popular e-commerce and online auction websites such as eBay and Amazon. For example, they have a *reputation system* where buyers can share their experience of and satisfaction with the goods purchased. Buyers are able to provide feedback and comments on the vendors and their services, thus creating a unique evaluation profile for each vendor (Europol, 2014). Using such reputation profiles, moderators can easily remove low-quality vendors, including scammers and providers of fake products and services. The presence of moderators in these websites increases the trust between buyers and sellers and the overall popularity of the forum. To enhance the trust between vendors and customers even further, several of these forums provide **escrows**. An escrow is a trusted third party who participates in the deals made between vendors and buyers in the underground forum who do not trust each other. The escrow makes sure that the money is paid only if the goods are delivered, reducing the possibility of fraud. Escrow services are offered in some hacking forums or are available as cybercrime-as-a-service offerings (see section 6.10).

Hacking forums are the primary marketplace used by criminals to exchange illegal assets and, as such, they play a significant role in the cybercrime ecosystem. Research studies of the underground economy of cybercrime have shown that the revenues and profits produced in the marketplaces operating within hacker forums are estimated to reach millions of US dollars (Holt et al., 2016; Holt, 2013). Other results show that revenues may reach up to $ 1 billion.[21]

3.3.2 e-shops

E-shops or “hacker shops” are a type of marketplace where illegal goods and cybercrime-as-a-service offerings are for sale. These e-shops are run by individual hackers or groups of hackers who want to sell a specific service or product. Such shops can also be found in the indexed web, served via bulletproof hosting providers and protected with anti-DDoS services. e-shops specializing in selling stolen credit cards, also known as carding shops, are a popular type of a hacker shop. Such shops facilitate the job of those who steal credit card information while, at the same time, enabling other criminals to find sources to finance their activities (Du et al., 2018).

3.4 Messaging Apps

Traditionally, cybercriminals used to interact via the Internet Relay Chat (IRC) protocol. IRC was one of the first “instant messaging” applications on the Internet that allowed multiple

[21]https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

parties to chat at the same time. To be able to communicate, users needed an IRC client and an IRC server to connect. Such IRC servers usually host multiple IRC channels. Channels are discussion forums that used for real-time group communication. Once users have joined a specific channel, they can either send broadcast messages to all connected users or communicate with a specific user, one on one, via private messages. IRC channels are not indexed by search engines and usually do not provide archives of previously sent messages and logs. These characteristics made IRC suitable for use by cybercriminals. Research has shown that there are IRC channels that contain general and specific discussions on hacking, tutorials, tips, malicious tools, external links to other sources of cybercrime assets, and information on how to enter other cybercrime communities (Du et al., 2018).

Although IRC is simple and easy to use, it has two main drawbacks: (i) it uses plaintext (i.e., no encryption), and (ii) all parties must be online simultaneously to communicate (i.e., no offline communications). To overcome the above (and other) limitations of IRC, cybercriminals today use a variety of modern applications that provide both real-time and asynchronous communication via encrypted channels. Such applications, named instant messaging applications, provide user-friendly interfaces, a variety of running environments and promise encrypted, anonymous and untraceable activity through their networks.

In recent years, research groups have observed an increase in the use of instant messaging applications for cybercriminal activities. Research results suggest that cybercriminals use popular instant messaging apps such as WhatsApp, Telegram, Discord, ICQ, Jabber, etc., and use lesser known apps to communicate, advertise illegal products and services, and exchange criminal assets.[22] Between January 2019 and January 2020, researchers from IntSights counted more than 56,800 Telegram invite links and 223,000 mentions of the application across cybercrime forums while, during the same period, Discord had more than 392,000 mentions in the same forums.[23] The increase in the use of instant messaging applications by criminals is probably related to recent LEA operations that took down popular marketplaces and forums. As an example, in 2017, the international Operation Bayonet shut down AlphaBay and Hansa, two of the most notorious Dark Web markets.[24]
Organised crime groups have also used platforms that were not popular with the public, as in the case of EncroChat. This platform was active from 2016 until June 2020, when the company ceased operations after police intervention. EncroChat provided modified mobile handsets that had their GPS systems, cameras and microphones disabled. These devices had pre-installed a custom operating system and the EncroChat messaging application, which was able to send and receive encrypted messages. EncroChat phones were not sold through regular retail outlets, but from a network of specific resellers who were involved in criminal activities. In July 2020, Europol reported on a joint investigation that enabled law enforcement to intercept and analyse millions of messages that criminals shared through the EncroChat network (Europol, 2020). These messages revealed numerous criminal activities, including violent attacks, corruption, attempted murders and large-scale drug shipments. At the time of its closure, EnroChat enumerated 60,000 subscribers and, as of 22 December 2020, the police had arrested more than

[22]https://www.reuters.com/article/us-cyber-summit-apps-messaging/criminals-try-message-apps-to-evade-dark-web-crackdown-report-idINKBN1CU2SS
[23]https://www.darkreading.com/risk/criminals-turn-to-im-platforms-to-avoid-law-enforcement-scrutiny/d/d-id/1338181
[24]https://www.europol.europa.eu/newsroom/news/massive-blow-to-criminal-dark-web-activities-after-globally-coordinated-operation

1,000 persons across Europe.[25] According to the French National Gendarmerie, 90 per cent of EnroChat users were involved in criminal operations, while the British National Crime Agency (NCA) reportedly found no evidence of non-criminal users on the platform.[26]

Other messaging platforms, such as Protonmail—one of the largest secure email services, developed by CERN and MIT—as well as Tutanota and cock.li email services, have been used by ransomware cybercriminals to communicate via an encrypted channel (Europol, 2020).

3.5 Anonymising services, the Tor network and Dark Web

Anonymity has been an important requirement in today's communications, as it helps protect privacy and facilitate free speech in repressed regions. Although anonymity is frequently desired by many people, the Internet has not been designed with anonymity in mind. For example, IP addresses, used for routing IP traffic, are frequently used in order to disclose the names of the people involved in a communication.[27] To enable anonymity over the Internet, researchers have developed a variety of techniques.

Onion routing is one of the most popular schemes to provide anonymity over a computer network. Onion networks encapsulate messages into multiple layers of encryption similar to the natural structure of an onion, which has many "layers", one inside another. Such networks have specific network nodes, called *onion routers*, that can decrypt a specific layer of encryption to reveal the next destination router, repeating until the final node, called the exit node, is reached. The exit node is the one where the plain message is delivered to its destination. The sender of the message remains anonymous, as each node only knows the identity of the previous node and the next node in the sequence and cannot decrypt all the layers of encryption, but only a specific one. Figure 2 illustrates the tor networks. Assume, for example, that Alice would like to send a message to Bob. To do so, she sends the message to onion router X, who sends the message to onion router Y, who sends the message to onion router Z who eventually sends the message to Bob. None of these routers has the information that Alice talks to Bob. Indeed, onion router X knows that Alice is talking to Y but it does not know that Alice is talking to Bob. Onion router Z knows that someone is talking to Bob, but it does not know that this someone is Alice. And finally, Onion router Y knows that there is some discussion going on, but doew not knows that Alice or Bob are involved in this discussion.

Tor is a circuit-based, low-latency, anonymous, communication service built upon the onion routing technique. As a second-generation system, it addressed many limitations of the original design by adding perfect forward secrecy, congestion control, directory servers and many more improvements (Dingledine et al., 2004). Although Tor (and similar anonymisation systems) can be used for legitimate purposes such as to protect freedom of speech in places where it is prohibited and to protect the privacy of people in places where this is desired, unfortunately, it can also be used by cybercriminals who would like to hide their identity. In this way, cybercriminals can communicate but they cannot be traced.

[25] https://www.bbc.com/news/uk-55402733
[26] https://www.ft.com/content/7006913f-be3d-49b5-8ba7-7c5b78b551b2
[27] IP addresses on the Internet are much like telephone numbers in the telephone network. Although telephone numbers do not immediately reveal the identity of the person who owns the number, they can be used to lead to this identity, possibly with the help of telephone companies.

In addition to enabling Alice to talk to Bob anonymously, Tor (and similar networks) can enable the anonymous hosting of web servers, what is frequently called as the **Dark Web**. Web servers hosted on the Dark Web cannot be (easily) traced. That is, the server hosting a web page in the Dark Web is protected behind an anonymisation network. This provides at least two benefits: (i) the real IP address of the web server cannot be found and (ii) the web server cannot be easily taken down by the appropriate authorities, because its IP address and its geographic location cannot be (easily) found. As a result, cybercriminals use the Dark Web to host illegal services and marketplaces, without fear of getting caught (at least easily). In addition to Tor, several other anonymising networks exist, including I2P[28], Freenet[29], etc.

Figure 2: The architecture of the tor anonymity network.

3.6 Deep web

Deep web[30] is a term frequently used to denote web pages and sources that are not indexed from standard search engines. There are many technical reasons behind this, but generally this "hidden" web is composed of pages that are dynamically generated and provided through private or limited-access sites. To reduce the accessibility to these sites, two main mechanisms are used:

- Requiring a password to access the pages. In this way, ordinary people (and search engines) are not able to access the web pages unless they can find the password.

[28] https://geti2p.net/en/
[29] https://freenetproject.org/index.html
[30] **Deep** Web should not be confused with **Dark** web.

- Hosting the pages on a server not accessed by search engines. That is, either the name of the server does not resolve to an IP address[31] or the IP address cannot be accessed (i.e., it is not routable) from the public Internet.

For example, consider your email. Typically, email (such as Gmail) is available only to authorised users via password-protected, dynamically-generated pages. Consequently, these web pages are not indexed by public search engines because they are not "reachable". As a result, although your email can be accessed by you on the web, it cannot be indexed by search engines, and thus, it is part of the "Deep Web". As another example, consider a company's confidential documents. These documents are usually hosted on servers that are not accessible from "outside" the company.

Cybercriminals may also make use of the Deep web to sell products and services outside the indexed or searchable World Wide Web, making their online "shops" harder for law enforcement to find and take down.

At this point, we should clarify some confusion about the "dark" web and the "deep" web. The deep web usually consists of websites that just do not contain public data, whereas the dark web consists mainly of shady or even illegal websites (in tor) whose owners go to great lengths to hide their data and geographic location.

3.7 Hosting services

Hosting services provide the infrastructure needed to host web servers and hence to publish resources online. Providers of web hosting services are able to make a website available to the world. Companies that provide such services mainly rent space on a web server and provide Internet connectivity to their customers. In other cases, such as domain name registrars, companies may provide their clients with DNS services.

HOSTING PROVIDERS OPERATE FROM COUNTRIES WITH LOOSE LAWS AND LOOPHOLES IN THE DOMAIN OF CYBERCRIME AND ILLEGAL INTERNET ACTIVITY.

Regular service providers have terms of service that disallow the hosting of illegal material and/or engagement in illegal activities. Once an abuse is reported or detected, the provider suspends the operations of the relevant client to eliminate the risk of (i) suffering damage to their reputation, (ii) being listed in global blacklists and having their network IPs being blocked by other providers and (iii) being accused of participation or involvement in illegal activities. Beyond these risks, ethical concerns and moral values could lead some providers to demand even more strict terms. To avoid suspension of their operations, cybercriminals may seek hosting services from smaller Internet service providers (ISPs) who do not have the resources (manpower and equipment) to successfully monitor and detect malicious activity in their

[31] For example, imagine that a company (let us call it company A) has a server named "secret.companyA.com". When we ask the DNS system for the IP address of "secret.companyA.com", no IP address will be returned.

networks. Cybercriminals also use providers with lenient terms of service. Such providers operate from countries with loose laws and loopholes in the domain of cybercrime and illegal Internet activity. Some Asian countries and former Soviet Union countries are in this category. In short, cybercriminals seek hosting services that will not easily be taken down as a result of illegal operations. Such hosting services are called *bulletproof hosting services* and are used for criminal acts. Bulletproof services are for sale in underground marketplaces as a cybercrime-as-a-service offering (see section 6.2).

3.8 Cryptocurrencies

Cybercrime usually involves monetary transfers. Indeed, buying, selling, payments of ransom—all involve transfer of money. Money transfers through the normal legitimate banking system are usually traceable and may eventually reveal the identities of the cybercriminals involved. On the other hand, cash transfers, though anonymous, do not easily scale to an online world. As a result, cybercriminals have to find (almost) anonymous ways to send and receive money electronically, ways that cannot be used to trace the cybercriminals' identities.

Cryptocurrencies are one way to provide this anonymity, which can hide the identity of cybercriminals who send and receive money.[32] Although several cryptocurrencies exist today, one of the first and most popular cryptocurrencies has been Bitcoin. Its wide acceptance has led to a phenomenal increase in its value, reaching a market capitalization of close to $1 trillion. Bitcoin is not strictly anonymous: it is pseudonymous. This means that we know which wallet is being used in each transaction—we just do not know who is the person behind each wallet. The equivalent with traditional banking is to say that we know which bank accounts are involved in transactions—we just do not know who owns each bank account. Although this form of pseudonymity protects to some extent the real identity of the people behind the wallets, it is possible that using some form of secondary information (such as when they sell Bitcoins to get real cash) to find the people who own the wallet and de-anonymise it. On the other hand, to protect their anonymity, cyberattackers may use Bitcoin to purchase other truly anonymous cryptocurrencies and then use those to purchase Bitcoins back. In this way, they can move in and out of Bitcoin, hiding their traces.

Cryptocurrencies are a key technical driver that facilitates the financial flows of cybercriminals.[33] A lot of money illegally earned from cybercriminal activities is laundered through cryptocurrencies (Europol, 2014). Cryptocurrencies are not used only for cybercrime. However, their market capitalisation[34], the rapid increase in their acceptance, and their anonymity (or pseudonymity) make cryptocurrencies an ideal vehicle for money transfers related to cybercrime. For more information on cryptocurrencies and their abuse by cybercriminals for money laundering, see section 6.1.

[32] https://cointelegraph.com/explained/digital-currencies-vs-cryptocurrencies-explained
[33] https://www.forbes.com/sites/vishalmarria/2019/02/04/how-cryptocurrencies-are-empowering-cybercriminals
[34] https://www.cnbc.com/2021/03/09/bitcoin-btc-value-exceeds-1-trillion-for-second-time.html

3.9 Availability of cryptography techniques

Cryptography and cryptanalysis (also called "crypto") techniques are widely used in cybercrime operations. Some examples include:

- secure protocols used to communicate with the target
- encryption of user data in ransomware
- obfuscation of code to bypass anti-virus and reverse engineering
- brute forcing of hashed passwords, and
- cryptocurrencies.

In the past, some of the algorithms behind cryptography were kept private for several reasons.[35] Back then, it was thought that if the algorithms were kept secret, this would provide better security against adversaries who would like to break these algorithms. Unfortunately, it was soon realised that hiding the algorithm resulted in worse security.[36] It was better (from a security perspective) to publicise the algorithm than to keep it secret. There are two main reasons for this:

- **When an algorithm is public, its weaknesses can be easily found and corrected**. Most algorithms (or their implementation) contain weaknesses that reduce their effectiveness. For example, they may contain a predictable random number generator, an easily guessable key, or even a plain software bug. Such weaknesses are not usually obvious and may take months (or even years) to be discovered, and only after they have been scrutinised by hundreds or even thousands of researchers. Once such weaknesses are discovered, they are fixed and lead to better future versions of the algorithm.
- **Cybercriminals usually find a way to steal an algorithm** that is kept secret. They may use extortion, they may have insider collaborators, or they may steal it. Thus, keeping an algorithm secret essentially means that it is kept secret only from the good guys, as the bad guys will eventually find a way to steal it.

Based on the above, it has become clear that cryptography should be public and easily accessible by all. Although some people may oppose this approach (and favour a "security through obscurity" approach), it appears that the cybersecurity research community clearly supports openness for cryptographic algorithms and implementations. Unfortunately, this openness also gives cybercriminals full and easy access to cryptography, and means that they can use cryptography for ransomware, for encrypted communication among themselves (to bypass monitoring by LEA), for anonymity (through Tor and similar networks), for hosting illegal services in the dark web, etc.

3.10 IoT and CPS

Over the past few years, we have been increasingly hearing the term "IoT" or "Internet of Things". This mainly implies that a multitude of devices (lots of "things") that we would not traditionally consider "computers" started to acquire computing and communication

[35] https://en.wikipedia.org/wiki/Crypto_Wars
[36] This approach is called "security through obscurity" and is usually frowned upon.

capabilities. Indeed, phones have already become "smart" (i.e., smartphones). Other devices follow closely: televisions are now becoming "smart"—meaning that they have computing capabilities and that they are connected to the Internet. Similarly, stoves, fridges, coffee-makers, security cameras, vacuum cleaners—all have started to become "smart" and join the IoT.[37]

Some of the most popular applications of IoT today are the following[38]:

- **Smart homes**: Hundreds of connectable devices are available out there and promise to make our homes smarter by providing automation and remote control extensions on ordinary equipment. Increasingly appealing to consumers is a new generation of lights, plugs, thermostats, cameras, bells, locks, air conditioners, heaters, kitchen appliances, vacuums and numerous other devices with smart features and Internet connectivity.
- **Smart cities**: As an extension to smart homes, we can envision IoT devices creating smart cities by handling problems of urban life and providing comfort with the use of technology.
- **Smart vehicles**: Vehicles have become increasingly more complex over time. Today's cars have many components that are software reliant and come equipped with sensors and devices that are connected online.
- **Wearables**: Smart devices designed to be worn on the human body. Consider smart watches, fitness trackers or sensors for purposes of healthcare and wellbeing.

Cyber-physical systems (CPS) are systems where software and mechanical elements are heavily intertwined along with minimal human interaction. CPS systems include industrial robots, collections of collaborating robots, manufacturing systems, autonomous cars, etc. CPS systems and IoT devices are principal components of the so-called Fourth Industrial Revolution (Industry 4.0) which represents the ongoing development of technologies in the field of manufacturing and industry.

However, along with the comfort and joy that these systems and devices have brought to our lives, serious threats and challenges have also emerged in the area of security and privacy. IoT devices have been created to be user-friendly, efficient, and able to better suit the needs and desires of customers. Unfortunately, in the majority of cases, security was not considered as a critical element in their initial design and during their development. The massive deployment of vulnerable IoT devices in the real world has exponentially increased the attack surface for cybercriminals. As the number of IoT devices increases, more and more endpoints connected to personal and enterprise networks are becoming subject to attacks.

The main threat in the IoT space is not so much the multitude of vulnerable devices out there, but mainly our perception of them. Indeed, when we see a smart vacuum cleaner, we essentially see a vacuum cleaner that has increased capabilities. When the cybercriminals see a smart vacuum cleaner, they have a different perception: they see a **computer** connected to a vacuum cleaner—and this computer can be attacked. In this aspect, IoT has created a paradise for cyberattackers: a computer connected to the coffee-maker, a computer connected to the vacuum cleaner, a computer connected to the light bulb, a computer connected to the refrigerator—and

[37] https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
[38] https://www.businessinsider.com/internet-of-things-devices-examples

all these computers are waiting to be attacked. And to make matters worse, these computers can do real damage in the real world: they can burn the food on the stove, let the meat spoil, turn the lights off, disable the heater in the middle of a snowstorm, lock the tenants out of their home, etc.

If we go past the issue of **perception** (which opens vast opportunities for cybercriminals), we encounter the issues of **standardisation** and **certification**. Indeed, several of the IoT devices are not certified with respect to cybersecurity. In this aspect, they may have vulnerabilities that we just do not know. To make matters worse, the lack of standardised protocols for all IoT devices just opens more opportunities for cyber attackers. Since several of these IoT devices are very lightweight, they communicate with the outside world (such as the cloud servers) through apps in smartphones. These apps, in turn, may weaken the security of the smartphone and its owner. Indeed, the more apps are loaded in a smartphone, the more likely it is to mount an attack against the smartphone owner through phishing, user tracking, requests for advanced (not needed) permissions, etc.

FORECASTS SUGGEST THAT BY 2024 WE WILL HAVE MORE THAN 35 BILLION IOT DEVICES WORDLWIDE

Several attacks on IoT devices have demonstrated recently the reality and gravity of these perceived threats. Apart from various device-specific IoT attacks, such as the one on Ring doorbells,[39] several large-scale attacks have been developed to leverage the advantage of large numbers of IoT devices. Such large-scale attacks started with the infamous Mirai botnet that generated DDoS traffic of unprecedented magnitudes (620 GBits/s). Once Mirai's code was released publicly, however, several variants of Mirai were quickly developed (e.g., Hakai, Mozi, etc.), thereby starting and exacerbating an unfortunate trend of triggering large-scale botnet attacks by exploiting IoT devices.

In 2019, more than 26 billion IoT devices were deployed around the globe.[40] One year later, the number of IoT devices had reached a total of 35 billion. By 2024, forecasts suggest that there will be more than 80 billion IoT connected devices worldwide.[41] This would be more than three times the number of devices in 2019. This substantial evolution in the IoT ecosystem requires better-designed privacy and security controls as well as new international standards for IoT technology.

3.11 Supply chains

"Supply chain" is a term used in commerce to describe the connections and the interactions that exist between several organisations, activities and resources, in order to develop and deliver a final product or service to a customer. This chain also defines the step-by-step procedure required to transform the product or service from its initial to its final state before reaching the customer. Any link in the supply chain is important in order to guarantee the integrity of the

[39] https://nordvpn.com/blog/ring-doorbell-hack/
[40] https://safeatlast.co/blog/iot-statistics/#gref
[41] https://www.juniperresearch.com/press/iot-connections-to-reach-83-bn-by-2024

final product and to successfully meet the customers' expectations in terms of quality and timing. If any of these links is broken, then the whole production will be broken and the reputation of the firm could be severely affected.

Cybercriminals take advantage of such circumstances to attack even the most security-conscious firms. The existence of major supply chains has dramatically increased the attack surface of a typical enterprise in the past few years. Modern attacks attempt to harm companies by targeting the less secure links in their supply chain. Typically, attackers determine the node in the chain that has the weakest cybersecurity and plays an important role in the supplier's network. Attackers steal sensitive data, infiltrate private networks and disrupt the services of a company by exploiting a third-party node that this company trusts and on which it depends. Such attacks are called **supply chain attacks** or **third-party attacks** and occur in almost all sectors of industry.

Supply chains help cybercriminals to conduct attacks on targets that have no direct responsibility for their own security, nor enough control to actively respond to these attacks. In recent years, regulatory frameworks and standards have been developed for compliance and risk testing for third-party vendors and suppliers.

Supply chain attacks have become more common. In its Internet Security Threat Report of 2019, Symantec stated that supply chain attacks had increased by 78 per cent between 2017 and 2018. Observed attacks since 2011 have abused utility and application software, providers of managed services and repositories for open-source projects used by many organisations.[42] Section 5.7 describes the most notable supply chain attacks observed in the past decade.

As mentioned above, the existence of supply chains basically increases the attack surface for cybercriminals. Indeed, cybercriminals now attack any link in the chain. To make matters worse, the steps of a supply chain may span several legal jurisdictions and may belong to several different partners, providing cybercriminals with a choice to select and attack the weakest link in the chain.

3.12 Cloud platforms

Modern technologies and their applications demand significant amounts of computing power, data storage and network bandwidth. In the past, companies used to acquire and maintain their own IT equipment and infrastructure. Unfortunately, this became increasingly complex as this infrastructure had to be maintained, updated and finally replaced. To make matters worse, unless they over-provision, companies could not adapt to demand surges in computer capacity needs. As a result, small and medium-sized companies could not easily maintain their own IT infrastructure.

To simplify procurement, maintenance and support, and to adapt to demand surges, cloud computing came into play. Cloud computing is a rapidly growing market that consists of computer resources and services offered by third-party providers, over the Internet, for purchase and use by everyone. Cloud platform vendors provide solutions to companies and individuals to build their infrastructures remotely and scale them on demand. Such solutions relieve companies from the task of purchasing, maintaining and managing hardware and software

[42] https://blog-assets.f-secure.com/wp-content/uploads/2021/03/30120359/attack-landscape-update-h1-2021.pdf

infrastructures on their premises. This responsibility and the relevant overheads have been transposed to the cloud provider. Other advantages of using cloud services are scalability, flexibility and agility. With a massive amount of ready-to-use resources, cloud customers can react quickly to the needs of their business by increasing or decreasing the size or power of their IT solutions accordingly. Typically, the customer notifies the provider of the change in demands, so that the provider can set up a new agreement and an adjusted payment plan, tailored to the new requirements.

As in the case of other technological achievements, cybercriminals can also benefit from the services of cloud providers to facilitate their attacks. They can use the cloud to host their illegal services, to exchange information, to launch attacks, etc. This provides cyber attackers with the following benefits:

- *On-demand computing capacity*. That is, cybercriminals do not need to purchase computers and place them in some building. They can rent this capacity with the click of a button.
- *Limited traceability*. If the computers of a cloud provider are used in cybercrime, LEAs will be able to find only the cloud provider, not the cybercriminal. Although the cloud providers have information about their clients, cybercriminals may use fake identities covering threir tracks.
- *Agility*. Even if the malicious activities of cybercriminals are discovered and their cloud account is closed, they can easily move to another cloud provider using fake credentials.

3.13 Social media

Over the past decade, people have been spending an increasing amount of time on social media.[43] Recent statistics indicate that more than 4.4 billion people use social media, close to 56 per cent of the worldwide population.[44] These people spend (on average) more than two hours a day on social media. This implies that a large percentage of everyday activities has moved online.

According to Wybo et al. (2015, 108) "[s]ocial media play a central role in the field of cybercrime, both regarding infringements on the individual properties and infringements towards physical persons". Furthermore, the current research indicates that the Internet provides a medium for both traditional and cybercrime and social media serves as the communication medium for Internet-based crime and criminal communities (Soomro & Hussain, 2019, 9). From this, it can be deduced that for both cyber-dependent and cyber-enabled

[43] According to the literature, the concept of social media is defined as follows:
"[T]he term 'social media' refers to a wide range of internet-based tools and uses allowing a large number of users and communities to share information, ideas or opinions in an interactive manner: blogs, microblogs such as Twitter, social networking sites such as Facebook and Wikis. ¬-- The main feature of social media is to be managed in a very decentralised way by the general public." (Wybo et al. 2015, p. 107)

[44] https://backlinko.com/social-media-users

crimes, social media plays a central role by providing various new opportunities and enhancing existing methods for perpetrators to engage into and commit cybercrime.

As social media permeate several aspects of human life, they are inevitably used in cybercrime as well. According to INTERPOL, social media are useful for researching potential targets, for making a first contact with people, for spreading particular types of information (e.g., authoritarian ideas, hate speech), etc. Social media enable cybercriminals to build an image (a "persona") appropriate for their purposes. If cybercriminals would like to approach young teenage girls, they create a social media teenager with similar interests. If they would like to approach single older men, they build a persona of an attractive female. Hidden behind these fake persona, cybercriminals find it easier to approach their victims, make a first contact and build rapport. Since social media provide some form of anonymity or pseudonymity, it is difficult for the victims to realise that the persona is the fake creation of a cybercriminal.

INTERPOL reports that "social media is increasingly used by criminals for online child sexual exploitation. Specifically, offenders within online child abuse networks are locating and contacting their victims on social media taking advantage of the global lockdown" and that "at the same time, the trade in child exploitation images has intensified"[45].

The following sections focus on how social media have been used to catalyse cybercrime.

3.13.1 Cyberstalking - sexting

EXPERIENCED INTERNET USERS ARE MORE LIKELY TO BE CYBERSTALKED!

Social media play a significant role in stalking through the Internet: cyberstalking. Indeed, Strawhun et al. (2013) suggest that the more time people spend on social media, the more likely they are to engage in cyberstalking. Similarly, Navarro et al. (2016) concluded that "there is a significant relationship between Internet addiction and cyberstalking in adolescents". It seems that, probably to no surprise, cyberstalkers spend an increasing amount of time on social media stalking (online) their victims. Cyberstalkers use social media to meet their victims. Fansher and Randa (2019) stated that 12.65 per cent of the individuals who reported victimisation noted an offender whom the victim initially met through a social media application. They suggest that the process of disclosing personal information over social media, under certain circumstances, represents a pathway to victimisation. They believe that social media are an entry point to that pathway. Berry and Bainbridge (2017) suggest that people who spend more time on social media have a higher likelihood of being cyberstalked. They found that experienced Internet users are more likely to be cyberstalked (or at least report that they are cyberstalked) compared to less experienced Internet users. Although this may be due to the fact that experienced Internet users spend more time online and, thus, are more likely to be found and stalked in cyberspace, it shows that even experienced Internet users are not immune to cyberstalking.

Similar patterns can be found in crimes related to sexting and revenge porn. Attrill-Smith and Wesson (2020) report that "more often than not" communication between the offender and the

45 https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

victim starts in social media. Through promises for wealth or a job delivered over social media, the offender tries to gain the victim's trust.

3.13.2 Deviant behaviour

Two properties catalyse deviant behaviour in social media: connectivity and anonymity.

MOST ONLINE HATE TODAY "IS NOT DISSEMINATED BY FORMAL HATE GROUPS BUT RATHER INDIVIDUALS OPERATING PERSONAL WEBSITES OR USING SOCIAL MEDIA PLATFORMS."
Costello and Hawdon (2020)

- ***Connectivity*** enables people to easily send their message to a broad audience, almost for free. Connectivity enables individuals to connect with people they do not know and with whom they would not be able to connect in real life in their traditional terrestrial environment. Online connectivity has less supervision from family and friends, which reduces the possibilities of someone in the physical world spotting deviant behaviour. Social media help people to easily find and connect with others with similar deviant ideas. This grouping gives them more incentive to continue their deviant behaviour.
- ***Anonymity***[46] enables people to speak with fewer inhibitions as there is no fear of revenge. Anonymity combined with the absence of physical proximity allows people to say things that they would not have said in a physical meeting and close proximity. This effect, frequently called the *disinhibition effect* (Suller, 2004), allows more radical ideas to be expressed.

Costello and Hawdon (2020) report that social media are used to disseminate hate speech. Although specialised hate groups have been operating online since the 1980s and well before the invention of the World Wide Web (see Daniels, 2009), Costello and Hawdon (2020) report that most online hate today "is not disseminated by formal hate groups but rather individuals operating personal websites or using social media platforms."

Lauger et al. (2020) suggest that gang members use social media to threaten peers, develop criminal identities and recruit new members. Holt (2020b) reports that organisations such as ISIS use Twitter to radicalise individuals and to convince them to travel from their countries to the Middle East region to join the war.

Gangs make extensive use of social media. Although online social media do not allow for physical violence, gang members use social media to deliver threats and intimidate people that may later culminate in physical violence in the real world. Social media can also be used to create an "image" for gang members – usually an image that projects toughness. For example, gang members show guns, drugs and disparage their adversaries by name (Lauger and Densley,

[46] The anonymity offered by social media is more like pseudonymity and not anonymity in the strong technical sense. That is, people may use a pseudonym, but careful research (or law enforcement work) may reveal their true identity. Thus, the anonymity offered by social media is better termed "perceived anonymity".

2018). Such activities in social media may bring immediate support – quantifiable support – through "likes", comments and feedback. In this way, social media strengthen deviant behaviour and gangs.

3.13.3 Scams

Social media have been widely used for various scam operations: phishing, fraud, etc. Offenders create fake social media accounts to approach their victims. To give legitimacy to these accounts, offenders may purchase "friends", post fake photos, purchase "likes" and create a seemingly legitimate, if not desirable, social media account. In this way, when victims search for them in social media, they will find misleading information that will trick them into trusting the offenders. Offenders often start what is called "romance scams". That is, using the legitimate and desirable online personality they have built, they approach emotionally vulnerable people, pretend to be interested in romance and then start getting money from their victims for a variety of reasons (Whitty, 2018; Whitty, 2019).

Kennedy (2020) reports that offenders frequently use social media such as Facebook, Instagram and WeChat to advertise "brand name" products that are counterfeit. The extent of the abuse of social media for fake brand name products is so high that some estimates report that as much as 50 per cent of sales of counterfeit cosmetic products is done through social media.[47]

In addition to using social media to springboard their illegal activities, perpetrators also target social media accounts of legitimate users. [48] Social media accounts of legitimate users often contain information including contacts accounts, and personal data that can be later used for targeted spear-phishing attacks.

3.13.4 Victimisation

Even when a crime is not committed online, social media are frequently used in various settings related to the crime itself. For example, social media are used by third parties (i.e., neither the perpetrator nor the victim) to comment on a crime committed offline. In some cases, such third-party use may result in repeated victimisation. Zaleski et al. studied online third-party comments on newspaper articles reporting rapes and sexual assaults. They found that almost all articles had at least one comment supporting the perpetrator and that a quarter of the comments blamed the victim. Fairbairn and Spencer (2018) reported that pictures of a sexual assault were shared online re-victimising the victim over again. This use of social media to re-victimise or to blame the victim has a significantly adverse effect on the victims. Social media can also be used for the benefit of the victim as they may attract national (or even international) attention to a crime that would otherwise be considered a small local crime by traditional media and stakeholders.

47

https://www.cosmeticsbusiness.com/news/article_page/Social_media_now_contributes_to_50_of_counterfeit_cosmetics_sales/143579

48 https://www.riskiq.com/blog/external-threat-management/q4-2017-phishing-roundup/

Moreover, Akdemir and Lawless (2020, 1665) argue that social media also connect with processes of victimization. Their research illustrated that "Internet users facilitated their victimisation through their online activities. Additionally, using insecure Internet connections and public access computers emerged as risk factors for both cyber-enabled and cyber-dependent crime victimisation. Voluntary and involuntary personal information disclosure through social networking sites and online advertisement websites increased the likelihood of being a target of phishing. Deviant online activities such as free streaming or peer-to-peer sharing emerged to increase the risk of cyber-dependent crime victimisation." By "deviant online activities", the authors refer to illegal online activities, such as viewing pornography, unauthorised access to someone's Internet communication and pirating media, and found these activities as the correlates of malware infection (Akdemir and Lawless, 2020, 1675).

3.13.5 Age and gender

The age aspect regarding the impact of social media in cybercrime and victimisation is significant as youth and adolescents are the groups using social media the most (Ganesan & Mayilvahanan, 2017. In their study, Almansoori, at al. (2021) analysed the characteristics of cybercrimes taking place in social media, it is argued that uneducated and poor people have more tendency to commit cybercrimes and people of the ages between 20 and 25 committed more crimes.

According to a recent study by Marttila et al. (2021), "both forms [online harassment and experiencing unwelcome advances] of cybercrime victimization are clearly more prevalent among younger people and those who use social media frequently". As young and adolescent people are the groups using social media the most for cybercriminal purposes. The majority of victims of cybercrime are young people. The reasons for victimisation of young people are: (i) they are the most popular group using social media platforms and (ii) they are often unaware of security aspects and risky behaviour online. Furthermore, cybervictimization is a notable threat especially for those already in vulnerable circumstances (Marttila et al., 2021).

In general, the research indicates that younger users, females and users with low educational qualifications are assumed to have weaker social guardianship against victimisation and therefore are in more vulnerable positions (Marttila et al., 2021; Keipi et al., 2016; Pratt and Turanovic, 2016).

3.13.6 Profit: a final note

Recent research suggests that social media are a very profitable platform for cybercrime underlying the fact that social media are not only convenient media – they are also very profitable. According to the "Web of Profit"[49]

- "social media-enabled crimes are generating global revenues of at least $3.25bn for the global cybercrime economy annually, including: illegal pharmaceutical sales (i.e.

[49] https://www.bromium.com/wp-content/uploads/2019/02/Bromium-Web-of-Profit-Social-Platforms-Report.pdf

prescription drugs) – $1.9bn; stolen data sales – $630m; financial fraud – $290m; cryptomining malware – $250m; romance/dating fraud – $138m";

- "reported crimes involving social media grew more than 300-fold between 2015-2017 in the US, while UK police data shows social media-enabled crime quadrupled between 2013 and 2018" and
- "social media platforms contain up to 20% more methods by which malware can be delivered to users – e.g. through updates or shares, add-ons, plug-ins etc. – than comparable sources, such as ecommerce, media or culture-orientated websites".

4 Human drivers of cybercrime

4.1 APPROACH AND METHODOLOGY 52
4.1.1 Rationale 53
4.2 INTRODUCTION 54
4.2.1 Offender profiling and cybercriminal motives 54
4.2.2 An introduction to profiling 56
4.2.3 Youth perpetration as a primary consideration 57
4.2.4 Gender and cybercrime 57
4.2.5 Cybercrime amidst Covid-19: profiteering from a pandemic 58
4.3 MULTIDISCIPLINARY APPROACH TO UNDERSTANDING CYBERCRIME 60
4.3.1 Criminology 61
4.3.1.1 Techniques of neutralisation, drift, and digital drift 61
4.3.1.2 Deterrence theory 62
4.3.1.3 Routine activity theory 62
4.3.1.4 Labelling theory 62
4.3.1.5 General strain theory (GST) 63
4.3.2 Psychology 63
4.3.2.1 Individual risk factors 63
4.3.2.2 Dark Tetrad 64
4.3.2.3 Theory of Planned Behaviour 64
4.3.3 Cyberpsychology 65
4.3.3.1 Anonymity online 65
4.3.3.2 Online disinhibition effect 65
4.3.3.3 Cyber presence and psychological immersion 66
4.3.3.4 Minimisation of status and authority online 66
4.3.4 Neuroscience 66
4.3.4.1 Addiction and excessive use 66
4.3.4.2 Impulsivity or low self-control 68
4.4 PROFILING CYBERCRIMINAL OFFENDERS FROM TYPES OF CYBERCRIME ACTS 68
4.4.1 Profiling hackers 69
4.4.1.1 Origin of the “hacker”, hacker ethos and hacker subculture 69
4.4.1.2 Hacker motivations 70
4.4.1.3 Hacker types and profiles 71
4.4.1.4 Routine activity theory: trade-offs between anonymity and notoriety 74
4.4.2 Profiling malware writers 76
4.4.2.1 Uses of malware 76
4.4.2.2 Motives of malware writers 78
4.4.2.3 Characteristics and traits of malware writers 78
4.4.2.4 Motives of ‘Malware-as-a-Service’ cybercriminals 79
4.4.3 Profiling ransomware users 80
4.4.3.1 The nature of ransomware and Ransomware-as-a-Service (RaaS) 80
4.4.3.2 Revisiting the ‘malice’ in malicious software: dark personality traits and extortionists 80
4.4.3.3 Other forms of extortive acts: sexual violence online 82
4.4.4 Profiling RAT users 83
4.4.4.1 Nature of RAT attacks 84
4.4.4.2 Motivation of RAT users 84
4.4.4.3 RAT users and voyeurism 84
4.4.4.4 Links to spyware, stalkerware and creepware 85
4.4.5 Online offender convergence settings 87
4.4.5.1 Gaming as a gateway 87
4.4.5.2 Hacking forums and hacker recruitment 88
4.4.5.3 Dark Web markets 89
4.4.5.4 Social media & cyber- dependent crime 91

4.5 CONCLUSION 92

"Computer crime and digital forensics is as much about the individuals involved in this deviant behaviour as it is about the technology... Therefore, research focusing on people is vital if we have any real hope of coming to grips with the phenomena of computer crime" (Rogers, Siegfried & Tidke, 2006, p. S119). The same is true in the defence of cybercrime as acknowledged by Jeong et al. (2019); "cybersecurity cannot be addressed by technology alone; the most intractable aspects are in fact sociotechnical. As a result, the 'human factor' has been recognised as being the weakest and most obscure link in creating safe and secure digital environments" (p. 338). Therefore, this chapter seeks to examine the lesser-known element behind the perpetration of technical crimes, namely the human element. The human element will be examined from the perspective of criminal profiling, i.e., what features of the crime are indictive of a specific characteristic or motive. Insights into the profile of cybercrime offenders is crucial to further knowledge in the field, given the affordances of the internet and its ability to conceal or obscure a perpetrators identity.

Criminal profiling an inductive reasoning process; it is the process of making inferences from the nature of certain criminal acts as to what are the likely traits of the perpetrators (Turvey, 2012). Modern criminal profiling is rooted in criminology, psychology and psychiatry and forensic sciences, and has often been used for the purposed of investigate purposes (Turvey, 2012). However, a branch of criminal profiling, namely Behavioural Evidence Analysis (BEA) seeks to "examine the behaviours and patterns in a particular offense and then make specific inferences about offender characteristics that are evident directly from crime-related behaviour. The purpose of BEA is to provide insight into criminal behaviour and to define or refine the suspect pool in a criminal investigation" (Turvey, 2012, p. 403). A criminal profile may encompass demographic or physical characteristics, behavioural traits, and psychological attributes. Criminal profiling or BEA is likely to become a burgeoning field with the ever-expanding cybercrime landscape. However, to date there are only two key texts, as identified in this review, that analyse in depth the criminal profiles and motives of perpetrators of different types of technical cybercrime (namely type 1 cybercrime Offenses, see section 1.4 for description of these offenses); both authored by Kirwan and Power (2012; 2013). Therefore, this chapter presents state-of-art knowledge and insights; using the existing knowledge base recent evidence and findings conducted within the last 10 years have been incorporated alongside the knowledge of new disciplines, namely cyberpsychology and cybercriminology.

4.1 Approach and methodology

This chapter aims to present a broad, multidisciplinary overview of some of the key theoretical perspectives that may be used to understand cybercriminality and cyber delinquency.

It identifies and analyses human drivers—that is, motives, characteristics, traits and psychological drives—that firstly enable and/or allow humans to act differently online, and secondly may contribute to the perpetration of harmful or cybercriminal behaviours. The research in this chapter is driven by two key research questions:

1. What do theories from key academic disciplines (criminology, psychology, cyberpsychology and neuroscience) tell us about the human drivers of cybercrime?
2. What do the tactics, techniques and procedures (TTPs) of cybercriminals tell us about the cybercriminal actor(s)?

The partners have prioritised collated sources for relevance and recent articles (after 2017) in the review. In total, they reviewed 144 sources. They found that work in this field falls into three categories:

- Theoretically driven
- Primary data:
    - Quantitative: Self-report questionnaires (general population studies, where offences may be disclosed)
    - Qualitative:
        - Interview or observational studies targeting offender populations only
        - Document studies using criminal records, reports or other documents
- Secondary data.

The partners have carefully selected the literature referenced within this chapter for being from reliable sources.

4.1.1 Rationale

This chapter explores human factors in relation to "Category 1" cyber-dependent crimes. As defined by the Council of Europe (COE) Budapest Convention framework, Category 1 cybercrimes[50] are "Offences against the confidentiality, integrity and availability of computer data and systems", including: "Illegal access", "Illegal interception", "Data interference", "System interference" and "Misuse of devices" (Council of Europe, 2001).

This chapter is divided into two main sections, in line with the two research questions. The first section (4.3) identifies key theories from four academic disciplines, namely, criminology (or cybercriminology), psychology, cyberpsychology and neuroscience. A multidisciplinary approach is key to a holistic understanding of the human drivers behind cybercriminal action and intent.

The second section (4.4) discusses the potential motives and drivers behind the tactics, techniques and procedures (TTPs) of five different cyber-dependent cybercriminal acts: namely, hacking, malware writing, use of ransomware, use of remote access trojans (RATs) and engagement in cybercriminal networks. This section infers connections between cyber-dependent crime, traditional crime, cyber-enabled crime and deviant behaviour. Since the work in this field is limited, this section cautiously explores what may motivate[51] cybercriminals to engage in specific types of cybercriminal acts.

[50] Since this chapter is predominantly focused on category 1 cybercrimes, there are cybercrimes that, while they may be mentioned, are not the focus of this chapter and fall outside the chapter's scope and aims, for example, online child sexual abuse or exploitation.
[51] It should be noted that some elements may be considered as unfounded, as this exploration of specific cybercrime motivations is based on hypothetical assumptions drawn from a non-exhaustive review of the current literature base.

4.2 Introduction

The global online audience is currently estimated to be over 5 billion[52] (Internet World Stats, 2021). Individuals are likely to behave in the virtual world in ways that they would not in the real world, with or without anonymity (Europol, 2014).

To tackle cybercrime, scholars and policymakers alike need to investigate and better understand what drives cybercriminality, when and for whom. Humanity is increasingly incorporating and depending on the Internet for an array of routine day-to-day tasks; accordingly, the shift to changing or new behaviours online and the opportunity for cybercrime to occur are also increasing and evolving (Sabillon et al., 2016). Unsafe behaviours online are common: this is arguably due to the level of awareness of safety online, personal choices in terms of protecting oneself online as well as the capacity to do so (Kranenbarg & Leukfelt, 2021). The steady increase in online users highlights the urgency for societies worldwide to deter and protect young people from engaging in risky behaviours online and the need to understand the criminological, neurological and complex psychological factors behind cybercriminal and cyber delinquent behaviours and the pathways that lead to cyber delinquency and cybercrime. Cybercriminal characteristics and human factors can differ exponentially from those of traditional crime (National Crime Agency, 2017), because of the anonymity, networks and subcultures that are quickly accessible online.

As online audiences increase, so does the prevalence of cybercrime and attacks in cyberspace. Since the majority of harmful situations encountered in cyberspace are human-enabled, this shift requires expanding the current climate of empirical and theoretical research to the more underexplored areas that are somewhat lacking in the literature. These include the application and adaptation of key criminological theories to cybercrime and the nuanced human and behavioural aspects of cybercrime. It is vital to build on our current knowledge and understanding of social and behavioural factors to successfully tackle cybercrime at its core, with targeted intervention and prevention initiatives. For instance, analysis of online behaviours has been used to predict cyber-bullying (Heirman & Walrave, 2012). The first conference on the Human Factors of Cybercrime was held in 2018, at the Hebrew University of Jerusalem, evidencing the significance of this area of research in the worldwide fight against online crimes (Bossler & Berenblum, 2019) and the long journey ahead that this entails.

This chapter presents a broad overview of key theoretical perspectives used to understand cybercriminality and cyber delinquency. In some cases, an applied shift has been introduced from classical theory to a hypothesised psychology of cybercriminality to explore the human factors behind cybercrime, alongside current literature that speaks to a specified sample of Category 1 cybercrimes. This chapter also considers motives and profiling in relation to Category 1 cybercrimes, as evidenced in the Budapest Convention.

4.2.1 Offender profiling and cybercriminal motives

“One of the basic assumptions of psychological profiling is that the offender’s method of operating (or modus operandi) is linked, among other factors, to his or her personality traits” (Schell, 2020, p. 697).

[52] https://www.internetworldstats.com/stats.htm

This section addresses the concept of offender profiling in cyber contexts. While attempts have been made to apply traditional theory to cybercrime and in the approach to empirical data analysis, the academic community must continue this journey to better understand the motives and drivers behind different types of cybercrime. Recent work has shown that curiosity and financial motives may be key (Powell et al., 2018). Lack of moral qualms, association with deviant peers and neutralisations have consistently been associated with a wide range of cyber-offending, and a perpetrator may engage in cybercrime for the "joy" of committing crime or simply as a shortcut to make tasks faster or easier (Finklea & Theohary, 2013). A secondary analysis study using US Department of Justice legal data found that almost 70 per cent of the cybercriminals included had been financially motivated to engage in criminal activity online (Neufeld, 2010), meaning that just under a third of the sample were driven by motivations other than personal profit. Neufeld reported the following motivations:

Neufeld's list of motivations
Financial Gain
Revenge
Reputation
Business Benefit
Hobby/thrill-seeking
Escape
Friend-family benefit
Hacktivism
Sex
Curiosity

Table 4: Cybercrime motives (Neufeld, 2010)

Financial gain is reported by Neufeld to be the leading motive for cybercrime, followed by revenge, and then by reputation. Similarly, financial gain, reputation or having a feeling of accomplishment were stated as clear motives for cybercrime by the National Crime Agency (National Crime Agency, 2017). Motives for cybercrime perpetration are complex and include human social factors and individual psychological traits; thus, it has been theorised that cybercrime is likely to increase with economic instability (Neufeld, 2010). Indeed, this has been shown to be the case with the recent surge in cybercrime reported during the pandemic (see section 4.2.3). When considering the amalgamation of human factors more broadly, we need to recognise that motives are complex, likely to be nuanced and fluid, and may not be as discrete as depicted in the above table. Further, the limitations and potential biases should also be acknowledged here: specifically, that these findings are drawn from a study including only convicted cybercriminals.

4.2.2 An introduction to profiling

Before cyberspace existed, forensic psychology, sometimes referred to as "criminal psychology" (Howitt, 2009), traditionally focused on violent or sexual crime or serious juvenile crime. Cyberpsychology has foundations in work published in the 1990s and is a fast-growing discipline. While some of the theories included under the umbrella of conventional psychology can be directly applied to cyberpsychology, the different nature and overall experience of cyberspace in comparison to traditional real-world crime and behaviours mean that this may not always be so (Kirwan, 2010). Essentially, it cannot be assumed that human behaviour online can be explained simply by applying offline behaviour to predict online behaviour.

As a discipline, forensic psychology carries notable public awareness and status, largely due to popular television programmes, such as *Criminal Minds*, which focus on techniques such as criminal profiling (Kirwan et al., 2012), and more recently forensic cyberpsychology, which was popularised in the US TV series *CSI: Cyber*. Offender profiling is one of many topics within forensic psychology. In cyber contexts, it is a key area of interest in the subdiscipline of forensic cyberpsychology (Connolly et al., 2016). Forensic psychology—more specifically criminal profiling techniques—has proven effective for identifying and prosecuting criminals in a wide variety of traditional crime cases globally. A forensic psychologist will use profiling techniques to make an educated guess regarding the characteristics of a cybercriminal (Tennakoon, 2011).

Methodologies for offender profiling in the context of cybercrime may utilise an array of tools, skills and digital forensics. As proposed by McGrew and Vaughn in 2006, an attack profile could contain useful information about motivation, breadth, depth, sophistication, concealment, attacker(s), vulnerabilities and tools (McGrew, 2006). However, because of its complexity, it has been noted that applying such methods in the context of cybercriminal investigations can be problematic in practice. For example, the barriers that cyber terminology and technology present can pose as logistical obstacles for academics, professionals, law enforcement and courtroom juries (Ciardhuáin, 2004). This may be more of an issue with category 1 and 2 cybercrimes (such as hacking and malware), in which a specific definitional language would need to be known, inclusive of the types of malware or hacks, in order for forensic psychology to be successfully applied and properly used. That being said, suggestions have been made to counteract lexical and definitional confusion, including using statistical probability in cybercrime cases in an attempt to better inform the general public (Carney, 2004). This could prove a useful tool for a range of cybercriminal offences in categories 1 and 2, including technical or sophisticated cybercrimes, but also category 3-5 cybercrimes (Budapest Convention on Cybercrime Classification, 2001) such as child sexual abuse material (previously termed 'child pornography'), online hate or copyright offences. Despite the long road ahead in using forensic psychology in the field of cybercrime, it has been argued that it could *"eventually be very useful in our efforts to solve the problem of online crime*" (Kirwan & Power 2012, p. 35). While it is acknowledged that extending the unique expertise and applied research that forensic psychology has to offer to the field of cybercrime does pose limitations, it is, however, an approach increasingly accepted in the field (Kirwan and Power, 2012) and carries the potential to better equip and enhance law enforcement processes and criminal proceedings in the evolving sphere of cybercrime. This chapter presents profiling of specific cybercrimes within section 4.4.

4.2.3 Youth perpetration as a primary consideration

Brewer et al. have opined that young people experience the Internet as a "potentially criminogenic medium" (Brewer et al., 2018, p. 115) and that 90 per cent of young people (between the ages of 13-17) use the Internet every day (Brewer et al., 2018). We know that most cybercriminals are male (Payne et al., 2019b) and many are young (Payne, 2020). Young people are using the Internet in their daily lives more and more and, in turn, may be increasingly at risk of committing certain categories of cybercrimes (Schell, 2020), such as criminal hacking (Aiken, Davidson & Amann 2016). Young people are familiar with the digital world, are tech savvy and are growing up with an increasing online presence (Payne, 2020). Online hobbies, such as gaming or surfing the Internet, online and offline peer groups and networks, or contextual societal factors have been found to be impactful when considering youth pathways into cybercrime specifically (Aiken, Davidson & Amann, 2016).

Further, and significantly when considering human factors, education and parental supervision have been highlighted in the literature as key in preventing cybercrimes (Lianos & McGrath, 2018). An example of this is the arrest of a "prodigy" child hacker in 2014, who was just 13 years old (Aiken, Davidson & Amann, 2016). The NCA has stated that more than 60 per cent of hackers start hacking before the age of 16 (National Cyber Crime Unit / Prevent Team, 2017). Studies have found that young people engaging in criminal behaviour online are not the same sociodemographic population as those engaging in traditional, offline crimes (National Crime Agency, 2017). For instance, cybercriminals, like traditional criminals, are likely to have weak family bonds and parental supervision; however, they tend to come from a broader range of social classes (Aiken, Davidson & Amann, 2016), including middle to upper-class in some instances, and own a family car (Lee & Holt, 2020). It has been argued that life course factors that have been found to reduce criminal activity historically, such as education and employment, may not have the same significance when we consider cybercriminal activity (Kranenbarg el., 2018).

The characteristics and broad human factors of a cybercriminal are likely to be associated with the crime being committed: for example, cyberbullying is an increasingly common characteristic of contemporary online communication. In a recent study that surveyed more than 300 cyber-active young people, an overwhelming 80 per cent reported engaging in this behaviour at least once (Lianos & McGrath, 2018).

4.2.4 Gender and cybercrime

"One of the most consistent and strong findings in criminology is that females commit much less crime and juvenile delinquency than males. This gender gap in law-violation is found using data on arrests, convictions, self-reported crime and victims' reports about offenders. It also appears to exist across nations and over time" (Heimer & De Coster, 2001, p. 2918). Whilst this is a well-established finding for traditional crime, and even though there is little empirical literature available to assess the gender-gap in relation to cybercrime, the same is thought to be true for cybercrime. There is a lack of systematic research focussing on gender in relation to cybercrime. Section 4.4. has our findings in relation to gender and specific cybercriminal acts. Some authors suggest that misogyny online may represent an even more important pathway than gaming or forums (discussed in section 4.4.5). Misogyny is also a key feature of these online environments (see Bada et al., 2021). These environments ascribe to typically male

ideals of mastery and dominance, often silence female voices or contributions, feature misogynic comments and humour, and are used to acquire knowledge about spying on female partners and sexual violence.

4.2.5 Cybercrime amidst Covid-19: profiteering from a pandemic

This section will briefly describe what cybercrime trends tell us about the characteristics, traits and psychology of cybercriminals through an exploration of findings from reports and studies that have accessed crime data during the pandemic. The 2019 IOCTA report highlights ransomware as the top threat, stating that, although the volume may have declined, ransomware attacks are in fact more detrimental, more targeted and carry longer lasting economic damage. Europol stated in late 2020 that the coronavirus pandemic had resulted in an "upward trend of cybercrime", whereby cybercriminals were taking advantage of the pandemic landscape and of society at its most vulnerable, especially in the contexts of phishing scams, malware and child sexual abuse material.[53] A recent analysis of the effects of the pandemic on cybercrime in the UK shows an increase of cyber-dependent crimes against individuals rather than organisations (Buil-Gil et al., 2021), including spikes in hacking of personal emails and social media and fraud related to personal online shopping.

The Covid-19 pandemic has spurred the expansion of the Internet and online resources into routine daily life. There has been an accompanying increase in malware, which may be motivated by financial gain or the intellectual challenge (Kirwan & Power, 2012). Essentially, amidst the pandemic, the Internet is adapting and evolving as a vital tool to serve humanity's everyday needs quickly and efficiently. This shift to and dependency on the Internet for school teaching, health support, pandemic information and groceries has led to an increase in vulnerable online users and, in turn, a global surge in various categories of cybercrime.[54] A recent example of a callous ransomware attack was carried out against the Irish healthcare IT system (Mehta, 2021) and involved the blackmail of 40,000 therapy patients after a hacker obtained access to their confidential records (Heikkilä & Cerulus, 2020). Another example of a cyberattack during the pandemic was that of a Finnish psychotherapy centre *Vastaamo* where a cybercriminal gang accessed vulnerable patients' records and proceeded to blackmail them. Eventually, the organisation filed for bankruptcy (Scroxton, 2021).

Either way, cybercriminals are taking advantage of the vulnerability of online users, especially in the context created by the pandemic and this mass, global fear that surrounds it, and are evidently able to adapt their techniques to fit the Covid-19 mould (Collier et al., 2020). Technological advances are accelerating exponentially and with this acceleration, comes an epidemic of online mis and dis information that often induces mistrust of professionals and authorities (Aiken, Farr & Witschi 2021). The World Health Organisation (WHO) has coined this information overload phenomenon as an "Infodemic," specifically describing the overload of information (including false or misleading information) in digital and physical environments during a global crisis, such as the recent Coronavirus pandemic. Following the outbreak of

[53] https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime
[54] https://www.europol.europa.eu/newsroom/news/covid-19-sparks-upward-trend-in-cybercrime

COVID-19, a surge of fake news, rumours, and hoaxes began to spread virally, which were disruptive both online and offline in terms of real-world choices and beliefs (Tasnim et al., 2020). Fake news spreads quickly and limitlessly via social media platforms, technical devices, online forums, and websites, and this unstoppable spread and the ramifications of this have been declared by professionals as extremely dangerous (Jokic-Begic et al., 2020). This is another key example of the risks emerging from the increased use of technology during COVID-19.

While reports of physical crime have fallen during the strictest lockdowns, during which citizens are quarantined, reports of online crimes have rocketed, with this unprecedented opportunity for increased device usage and for cybercriminals to attack (Buil-Gil et al., 2021).

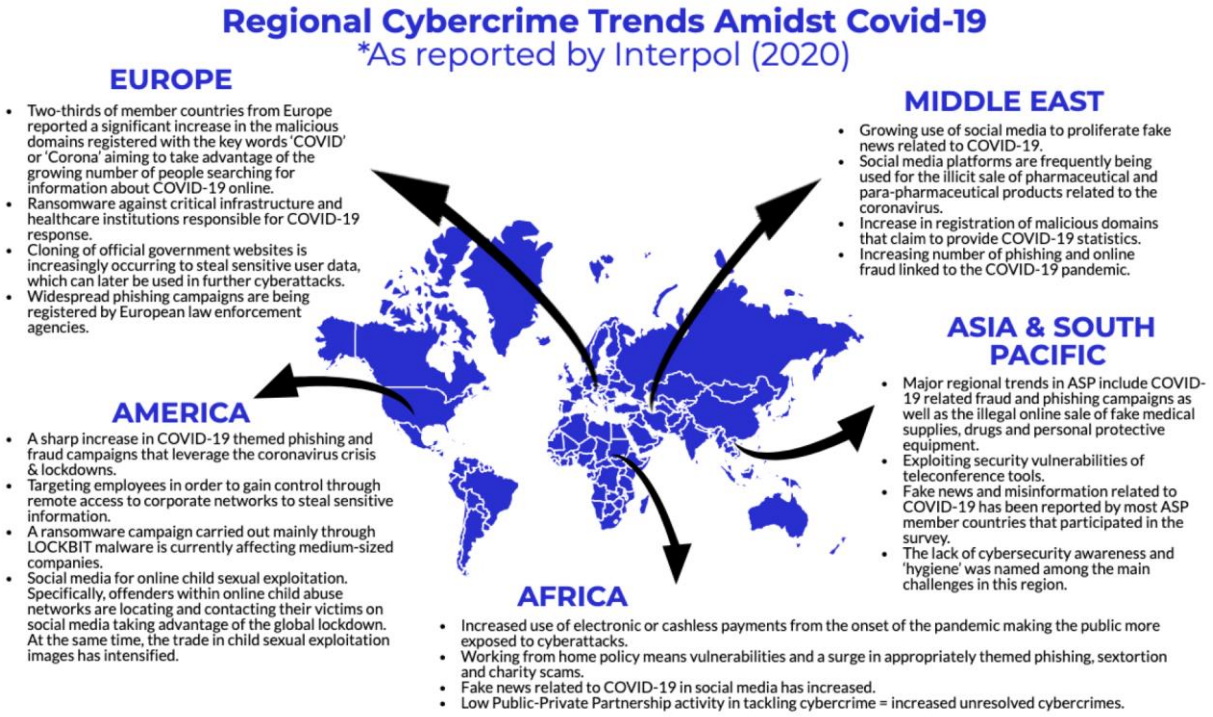


Figure 3: Regional cybercrime trends during the pandemic (INTERPOL, 2020, p6-7) visualised by UEL on a global map

As noted in the infographic shown above, there have been some communal global trends in cybercrime during the pandemic, especially financially motivated cybercrimes such as malware and phishing. The world has experienced an unprecedented rise in online crimes against children during the pandemic. In 2020, NCMEC reported a disturbing spike in *CyberTipline* reports of online enticement, with the rate of these types of incidents increasing by 97.5 per cent in comparison to 2019 (National Centre for Missing and Exploited Children, 2020). This is probably partly due to children spending more time online worldwide, especially during the strictest lockdowns.

Despite the surge in online crimes since the coronavirus outbreak, there is a paucity of literature that aims to better comprehend the motives and human factors behind pandemic-related cybercrime. It is worth questioning and further exploring what this surge in cybercrime is telling us, whereby cybercriminals are essentially using the catastrophe for personal financial gain. Unfortunately, when they see politicians benefitting their donors with untendered contracts,

cyber delinquents do not have good role models. Further, this exponential increase in cybercriminal activity is arguably heightened during pandemic lockdowns by an increase in risk factors identified in "Pathways into cybercrime", such as greater unmonitored device usage, boredom and isolation (Aiken, Davidson & Amann, 2016).

4.3 Multidisciplinary approach to understanding cybercrime

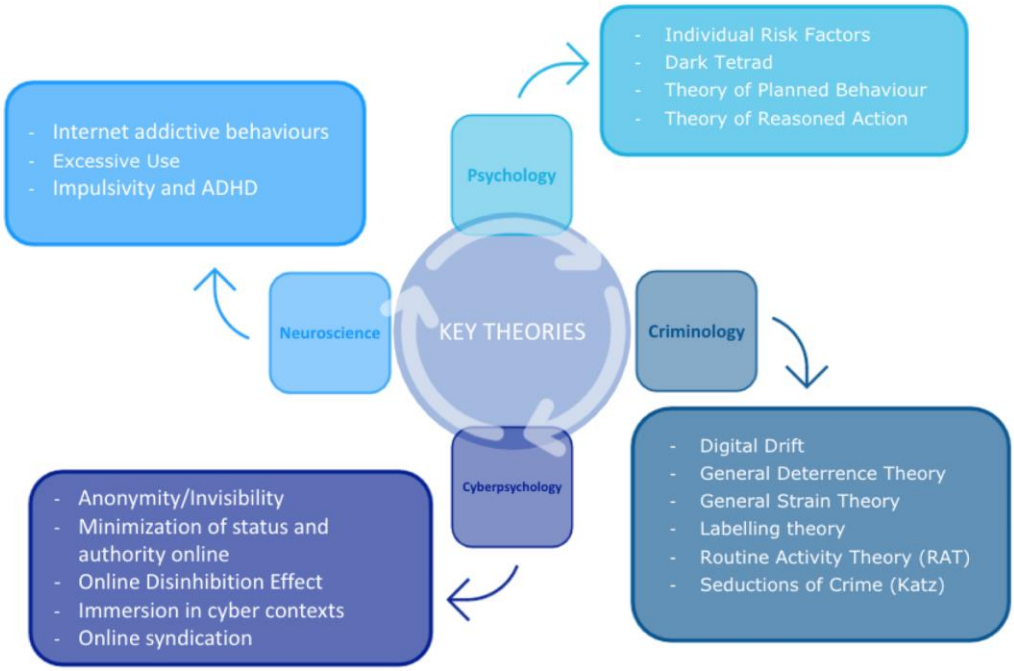


Figure 4: Taking a multidisciplinary approach

"Arguably, academic investigation of criminal behaviour in cyberspace requires interdisciplinary efforts in a practical sense, and transdisciplinary theoretical perspectives in an exploratory context" (European Cybercrime Centre, 2014).

Adopting a multidisciplinary approach allows for a more holistic understanding of the human factors behind cybercrime by cross-fertilising a sample of key classical and adapted theories that fall within overarching crucial disciplines, namely, criminology, psychology, forensic psychology and neuroscience. The above figure presents some of the key theories and disciplines explored within this chapter. The meeting of theories can lead to new findings: for instance, criminology seeks to provide explanatory value regarding criminal behaviour, and breakthroughs in the field are likely to help to inform practice and studies exploring the psychology of cybercrime (Europol, 2014). As depicted in the diagram above, this chapter includes relevant theories that fall within criminology, psychology, cyberpsychology and neuroscience, within sections 4.3.1 to 4.3.4. Where possible, a "case study" box or a separate

application of the theory to human factors of cybercrime and cyber delinquency has been included to underpin the significance of these traditional theoretical approaches to the ever-growing and evolving world of cybercrime and cyber delinquency. Human behaviour may be influenced by such cyberpsychological factors as environment, anonymity, disinhibition, minimisation of status and authority, along with the effects of normalisation[55] and socialisation[56] in technology-mediated environments (Aiken, 2016). Given the synthesis of factors at play, and the ever-changing world of cyberspace, a multidisciplinary approach carries the potential to strengthen understandings and potentially to develop new theories and approaches regarding the human factors of cybercrime.

4.3.1 Criminology

4.3.1.1 Techniques of neutralisation, drift, and digital drift

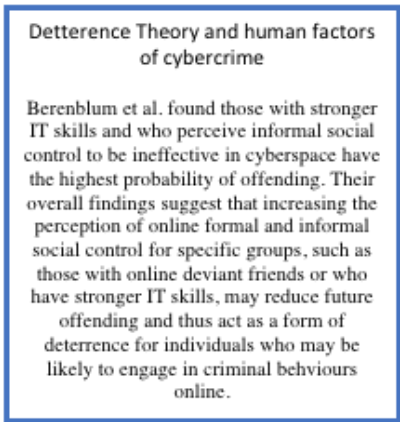
An Empirical Study conducted in Australia focusing on digital drift found some congruence between online and offline delinquency, and suggested specific patterns in the pathways into problematic online behaviours. Participants reported concerning levels of harmful online exposures, although were not necessarily aware of the impact of these. More research is needed/ (Brewer, Cale, Goldsmith, & Holt, 2018)

The engagement or drift into cybercrime or cyber delinquency by "normal" youth has been proposed as something that may be "easy to do" and "almost accidental" (Goldsmith & Wall, 2019). The foundational concept of "drift" originates from the work of early criminologists such as Matza (2009/1964), who suggested that delinquent values are in fact held by the majority, but are often suppressed through socialisation and learnt skills and behaviours in the context of social norms. Neutralisation theory dictates that criminals may develop explanations for their behaviour that they may not previously have regarded as morally acceptable. When applied to the cybercrime landscape, an offender may explain their illegal downloads as not being directly harmful, partly due to the anonymity and the distant nature of cyberspace (Kirwan & Power, 2012). Together, the drift into cybercrime and the neutralisation of risky online behaviours may arguably facilitate a young person's descent into cybercriminality.

[55] When such forces come together, as they do every day in cyberspace for many troubled people, morality is irrelevant. Consequences are not factored in. Reality becomes deeply distorted and the individual acts out, propelled by dark impulses that have been inspired, confirmed, normalised and reinforced over and over by other people, and experiences, and extreme content online.

[56] The Oxford Dictionary of Psychology defines socialisation as "the process, beginning in infancy, where one acquires the attitudes, values, beliefs, habits, behaviour patterns, and accumulated knowledge of one's society . . . and modification of one's behaviour to conform with the demands of the society or group to which one belongs." Here's how it works: A group or community assimilates new members by familiarising and educating them in its ways. Online, familiarisation can be formal or informal. Norms and rules can be communicated explicitly or implicitly. Successful socialisation is marked by acceptance. In social psychology, we call this "norming". As members of a group start to bond, a group identity forms. This is part of the norming stage of group development, which is a natural part of socialisation.

4.3.1.2 Deterrence theory



The multidisciplinary volume of literature on cyber deterrence is increasing steadily, as is the adoption of deterrence techniques in cyberspace as a tactic to fight an array of online crimes (Maimon, 2020). The very foundation of the theory dictates that humans are generally rational decision-makers, whose actions reflect a natural intrinsic desire to obtain the maximum pleasure but to avoid personal pain. Ultimately, a fear of punishment may prevent the public from committing crime, but equally deterrence measures may also serve as a tool to reduce recidivism among the previously convicted (Beccaria, 1963). Scholars have identified some fundamental issues with the application of deterrence theory to cyberspace, predominantly due to the anonymity and far-reaching nature of the World Wide Web (Nye, 2017). It has been argued that deterrence theory cannot be applied to cyberspace or relied upon to reduce cyberattacks (Lupovici, 2011). Cybercriminals are increasingly aware of the opportunities to avoid detection by law enforcement and of the low prosecution rate for cybercriminal activity in comparison to traditional crime, which weakens the premises for cyber deterrence and poses obstacles for successfully deterring cybercriminal activity. Conversely, a recent review of system trespassing has argued that surveillance and deterrence tactics in cyberspace can help to reduce the scope and prevalence of illegitimate activity (Maimon, 2020).

4.3.1.3 Routine activity theory

Routine activity theory originated in the 1970s and, when applied to cyberspace, may help scholars to better understand the culmination of factors that lead to cybercrime perpetration and for whom. Grabosky states that, although Routine Activity Theory was initially developed for traditional street crime, it is still relevant in the context of cybercrime *(*Grabosky, 2001). This theory highlights the opportunistic nature of crime. When applying it to cybercrime, the physical world is swapped for the world of cyberspace. Routine Activity Theory has been used in recent years to predict potential forms of online victimisation (Holt et al., 2020). Predictors of victimisation included gender, age, level of education and device usage. For more on the history and application of Routine Activity Theory, see section 4.4.1.4.

4.3.1.4 Labelling theory

Labelling Theory is considered as a sociological criminal perspective, within which the macro societal reactions are highlighted as a crucial factor behind criminal perpetration (Carrabine et al., 2009). According to Labelling Theory, a label with criminal connotations may be manifested by criminal behaviour and a criminal career. Essentially, Labelling Theory predicts that self-identity and the likelihood of committing a crime may be influenced—or even determined—by being type-casted and labelled, as an individual conforms to society's expectations of them. When considering the human factors of cybercrime, Labelling Theory has an interesting application, heightened by the definitional ambiguity surrounding online

crimes and the notion that some cybercriminals do not even themselves identify as criminals (Neutralisation Theory, as introduced in section 4.2, is relevant here). Further, the notable variety and subjectivity of cybercriminal labels when it comes to online perpetration may pose questions about the application of this theory to cybercrime (Kirwan & Power, 2012). Labelling Theory has been applied to cybercrime perpetration in recent years (Payne et al., 2019a) to further conceptualise various aspects of cybercrime prosecutions in the United States. While primary deviance may be a rejection of societal norms, secondary deviance refers to a deviant behaviour that is a result of being publicly labelled whether by the media, family or community. A linkage can be made here to section 4.4.1 on Profiling hackers, whereby hackers may partake in various subcultures and labels assigned to hackers, which may influence their online behaviours and choices.

4.3.1.5 General strain theory (GST)

Traditional criminological macro level societal theories can be applied to the field of cybercrime (Howitt, 2009). In this perspective, crime can be argued not to be a result of an individual, but rather as a pre-existing societal consideration on a larger scale (Kirwan G. & Power, 2012).

According to Agnew (1992), strain is based on the presence of three distinctive components:

1. failure to achieve a goal
2. the existence of harmful impulses
3. the removal of positive impulses.

In this case, where shared communal goals (such as financial goals) entrenched within the rhetoric of a society are unobtainable for individuals, they may resort to achieving such goals via illegal means. There is evidence to support the notion that strain leads to cyber offending. This link has been mostly explored in relation to cyberbullying but has also been found in relation to cyber dating abuse (see Hay and Ray, 2020, p. 591-593). Strain in relation to crime is a new concept in criminology; traditional strain theories were proposed by Merton in the late 1960s (Merton, 1968).

4.3.2 Psychology

The impact of technology on youth development is an area of great interest in the field of psychology (Europol, 2014)

4.3.2.1 Individual risk factors

Aiken, Davidson and Amann report stakeholders' experiences in their paper "Youth Pathways into Cybercrime", and risk factors such as having low self-esteem, vulnerability and being socially isolated (Aiken, Davidson & Amann, 2016). Personality traits can play a part in the likelihood of both cybercrime perpetration and victimisation (Mikkola, 2020). Linkages have also been made between childhood socialisation, impulsivity and low self-control online, suggesting that early life may play a role in cyber deviance and so be considered as a risk factor (Schell, 2020). Experts in the field have started to identify and map risk factors such as childhood abandonment, narcissism, poor anger management and inadequate stress-coping mechanisms, but there is a long way to go before the risk factors are better understood. The

pathways and individual factors are considered as trajectories of cyber misconduct that may help to answer why and how one is drawn into deviant or illegitimate activity in cyberspace (Aiken, Davidson & Amann, 2016).

Other factors (Schell, 2020) may, for example, include:

- Having a passion or skill for technology
- Feeling isolated and having a desire to gain reputation and self-esteem possibly lacking in the physical world
- Being part of a peer network that normalises deviant online activity.

Based on the above, policymakers should prioritise intervention and prevention programmes that aim to support young people at risk of drifting into cybercrime perpetration or to mobilise curious and technologically-skilled teenagers in legitimate activities, while positive role models, capable guardians, and support networks are key to preventing cybercrime.

4.3.2.2 Dark Tetrad

Paulhus and Williams (2002) identified the Dark Triad (i.e., Machiavellianism, narcissism and psychopathy), a meeting of traits reflective of what might be deemed as callous or unpleasant personality characteristics. The predictive ability of the Dark Tetrad (Machiavellianism, narcissism, sadism and psychopathy) was statistically applied to explore cyberbullying, and the results were significant (Brown, 2019). This research makes an original contribution by demonstrating the behaviour of different groups, and their subsequent willingness to engage in cyberbullying. Furthermore, female participants score less than their male counterparts across all four traits. The Dark Tetrad has been considered as a modern-day psychological approach to evil (Book et al., 2016).

4.3.2.3 Theory of Planned Behaviour

At its core, the Theory of Planned Behaviours (TPB), which links one's behaviours and beliefs, has been applied in the context of adolescent cybercrime and deviancy, to investigate the perpetration of adolescent cyberbullying (Heirman & Walrave, 2012) and sexting (Walrave et al., 2014). TPB modelling accounted for 33.2 per cent of the variance in relation to self-reported cyberbullying perpetration and 44.8 per cent of the variance in relation to the intention to cyberbully (Heirman & Walrave, 2012). In particular, sub-constructs of "cyberbullying attitudes" and "behavioural intention" were strongly correlated with intention to cyberbully; sub-constructs of "perceived behavioural control" and "subjective norm" were significant but less strongly correlated. Essentially, one's perceived ability to carry out a behaviour may help to predict online behaviours. The predictive ability of TPB in understanding cybercrime has been explored. Yao and Linz (2008) used the TBP framework to investigate online behaviour, making an original contribution to the field and demonstrating that more research is needed in this area.

4.3.3 Cyberpsychology

Cyberpsychology is a field that falls within applied psychology. Cyberpsychologists focus on the impact of emerging technology on human behaviour and study the following areas:

- Internet psychology
- virtual environments
- artificial intelligence
- intelligence amplification
- gaming
- digital convergence
- social media
- mobile and networking devices.

Although the discipline is relatively new, there are over 30 peer-reviewed journals publishing in the cyber behavioural sciences and more than 1,000 yearly articles (Europol, 2014). Undoubtedly, these numbers have increased over the past six years.

4.3.3.1 Anonymity online

"The anonymisation techniques used in parts of the Internet, known as Darknets, allow users to communicate freely without the risk of being traced. These are perfectly legitimate tools for citizens to protect their privacy. However, the features of these privacy networks are also of primary interest to criminals that abuse such anonymity on a massive scale for illicit online trade in drugs, weapons, stolen goods, forged IDs and child sexual exploitation" (Aiken & Mc Mahon, 2014).

The invisible and anonymous nature of various elements of cyberspace allows people to behave in ways that would be unlikely in the real world. Essentially, individuals will take advantage of the invisibility the Internet affords them (Liggett et al., 2020). Visual anonymity online may play a crucial part in lower self-awareness or self-reflection (Joinson, 2001) and may mean that people might alter their behaviour when mediated by technology. An example of this might be cyberbullying or trolling. Anonymisation tools can be loosely categorised (Aiken & Mc Mahon, 2014) as follows:

1. (simple) proxies,
2. virtual private networks (VPNs)
3. dark nets

These tools are commonly and frequently adopted by Internet users, and it should be highlighted that the use of these tools does not always necessarily point to illegitimate online activity.

4.3.3.2 Online disinhibition effect

Individuals may disclose certain information or act out more on the Internet than they would in person; however, both personalities or behaviours are part of one's "self" and not totally

separate from the surrounding environment. Six factors can interact with each other to create the online disinhibition effect:

1. dissociative anonymity
2. invisibility
3. asynchronicity
4. solipsistic introjection
5. dissociative imagination
6. minimization of authority

Personality variables are also likely to influence the extent of online disinhibition (Suler, 2004, p. 321).

The effects of anonymity and lack of eye contact online have been found to be contributors to negative or toxic online disinhibition (Lapidot-Lefler & Barak, 2012).

4.3.3.3 Cyber presence and psychological immersion

The impact of digital technologies on human presence and emotion is a growing area of research. An empirical study (Riva et al., 2007) aimed to explore the effects of virtual reality (VR) experiences on users and the feeling of presence in the computer-generated world. The results confirmed VR as an effective medium for presence and emotion—for instance, the interaction with "anxious" and "relaxing" virtual environments produced anxiety and relaxation within the computer-generated worlds included in the study. The levels of presence and immersion experienced by users may be linked to a variety of factors (Takatalo et al., 2008).

4.3.3.4 Minimisation of status and authority online

The lack of visible policing online may enable cybercriminal and cyber delinquent behaviours in cyberspace (Suler 2004). Suler uses the example of real-world visible status and authority reminders, such as uniforms worn by police officers or other authority figures, that can act as daily societal reminders of status and power and prevent illegitimate activity. However, these visible reminders are largely absent in cyberspace. While fear of punishment may prevent criminal behaviour from taking place in the real world, people may be more likely to misbehave online, where there is no centralised or visible control. There are similar elements discussed here that are present in routine activity theory (see section 4.4), such as the lack of guardianship online.

4.3.4 Neuroscience

Neuroscience is the study of the brain, which might be considered as the most complex and nuanced system that exists in the world as we know it (Rosenzweig, 2002). A branch of neuroscience named behavioural neuroscience (or sometimes called biopsychology) aims to interpret the key learnings of neuroscience to understand human behaviour, mood and motives (Rosenzweig, 2002). Thus, it is a key discipline in exploring the human factors behind cybercrime and encapsulates the notion of agency and free will when determining pathways into crime as well as criminal responsibility.

4.3.4.1 Addiction and excessive use

There have also been correlations made between Internet addiction and cybercrime perpetration (Schell, 2020). The notion of computer addiction was initially discussed by experts in the 1970s

and was picked up by mainstream society shortly after in the 1980s (Schell, 2020). During this latter period, concerns relating to the increased usage of computers began to surface. Specifically, potential detrimental effects of excessive use (such as negative impacts on social life and work performance) were published in a notable article in 1989 (Schell, 2020; Shotton, 1989). Three subtypes have been proposed since: excessive gaming, excessive online communications and preoccupation with sexually driven online activities (Block, 2008). It is argued that each subtype shares four components, as illustrated in the figure below.

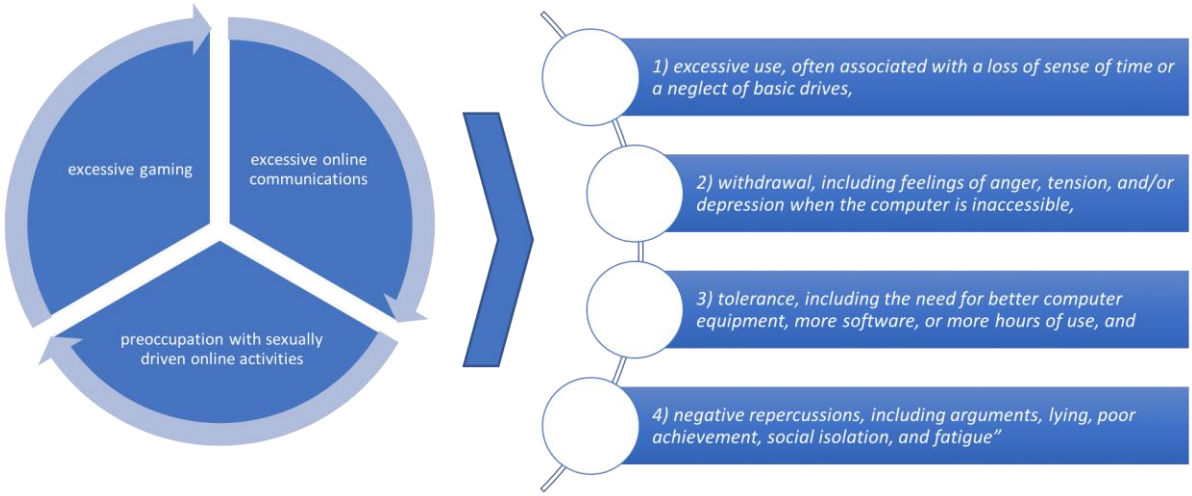


Figure 5: Block's proposed excessive use framework presented visually by UEL

When considering the human factors behind cybercriminality, the significance of excessive device use and the subsequent possibility of Internet addiction cannot be underestimated, as these have been consistently argued to be crucial human factors (Aiken, Davidson & Amann, 2016). Excessive use of devices has also been identified as a risk factor for becoming a victim of cybercrime, including specific use of the Internet: for instance, browsing, chatting, gaming and engaging in online forums (Leukfeldt & Yar, 2016).

The possibility of a related addiction to cybercrime has been proposed, and it has been argued that individual traits (such as Internet addiction) may heighten one's likelihood of committing both traditional and online crime. Aiken presented a real-life case-study that demonstrates the dangers of Internet addiction and excessive use:

> Cyberpsychologist Professor Mary Aiken presents the 2010 real-world case of Alexandra Tobias, a 22-year-old mother in Florida who called 911 to report that her 3-month-old son Dylan stopped breathing. Tobias was playing "FarmVille" on her computer and lost her temper when the baby's crying distracted her from the Facebook game. The mother picked up her baby and shook him violently, which resulted in hitting his head on her computer. Dylan was pronounced dead at the hospital from head injuries and broken legs. Tobias was sentenced to federal prison for 50 years for second-degree murder. (Aiken 2016, pp. 45–46)

4.3.4.2 Impulsivity or low self-control

Although more research is needed, scholars have argued that an individual's ability for self-control is established during periods of child socialisation and childhood experiences (Schell, 2020) and efforts have been made to explore low self-control and cybercrime. Impulsivity is defined as "a personality trait characterized by the urge to act spontaneously without reflecting on an action or its consequences, this trait has been attributed to important psychological processes and behaviors, including self-regulation, risk-taking, and poor decision-making" (Schell, 2020, p. 689). Impulsivity has been connected to crime, and scholars have proposed that excessive Internet use or Internet addiction is driven by impulsive behaviour (Schell, 2020). Impulsivity may encapsulate the urge to act spontaneously with no thought of consequences. Personality traits, including low self-control, that are acknowledged to influence cybercrime perpetration have also recently been linked to a higher likelihood of being victimised online (Holt et al., 2020) as a result of personal characteristics and online behaviours.

Low self-control has been linked to Internet addiction. Findings have indicated that participants reported enjoying socialising online more than in real life, with reported increases in sense of community, entertainment and belonging. However, these positive experiences of Internet use are accompanied by feelings of depression and anxiety after excessive use (Schell, 2020). This may be linked to Block's excessive use framework, presented above in Figure 6, whereby excessive internet use results in:

- Neglect
- Withdrawal
- Anger
- Social isolation
- Fatigue

4.4 Profiling cybercriminal offenders from types of cybercrime acts

Cybercriminal profiling examines the potential motives and drivers behind the tactics, techniques and procedures (TTPs) of cybercriminal actors. There are many ways in which category 1 cyber-dependent crimes can be conducted and many ways in which specific goals can be achieved. However, the nature of the act that the cybercriminal chooses may reveal information about the perpetrator. In section 4.4, we explore five types of cyber-dependent cybercriminal acts to consider the following question: what does the cybercriminal act reveal about the motives, traits, characteristics, personality and human drivers of the cybercriminal actor(s)?

Whilst outside the scope of this review, it important to note that Behavioural Evidence Analysis (BEA) has been applied to other categories of cybercrime, an example of which is the possession and distribution of OCSEA materials, using P2P networks (Al Mutawa, Bryce, Franqueira, & Marrington, 2015). In this research study, 15 cases of possession or distribution of OCSEA materials was examined. It was found that there was no consistent demographic profile of offenders, however, this may have been due to the limited sample or the context in which the study is conducted. For example, studies that examine a larger sample of cases in the US or UK find that most offenders are Caucasian. Overall, most studies find that demographic profiles vary, in relation to education, age, employment and socio-economic status. However,

most studies find that this group of offenders tend to not have a criminal history and are not typically violent offenders. Behavioural profiles however, show greater utility in relation to this offender group, Krone (2004) for example developed a nine category typology and Al Mutawa et al (2015) were able to demonstrate significant commonalities in offender behaviour within this group. However, as this offender group is outside the scope of the review, these offender profiles will not be examined in depth within this report.

First, we discuss hacking (used as a general term) in regard to the hacker ethic and hacker subculture; hacker motives; different types of hackers; and the trade-offs between anonymity and identity for hackers from the perspective of routine activity theory. Then, in line with the topics discussed in the wider report, the second subsection discusses a specific form of category 1 cyber-dependent crimes, namely, the use of malware. With respect to malware, we explore four topics: the uses of malware, the motives of malware writers, the characteristics and traits of malware writers and the motives behind "malware-as-a-service" (MaaS).

In the following two subsections, we explore the literature on two types of malware that are thought to significantly diverge in terms of motive. In the third subsection, we explore three topics on ransomware: the nature of ransomware and ransomware-as-a-service (RaaS), the malicious nature of ransomware users, cyber-dependent crimes and other forms of cybercrimes where extortion is used for financial gain or other motives. In the fourth subsection, we explore four topics on the use of remote access trojans (RATs): the nature of RAT attacks, the motivation of RAT users, the links between use of RATs and voyeurism, and the links between RATs and purpose-designed surveillance apps (spyware, stalkerware and creepware).

In the final subsection, we explore the literature on online offender convergence settings. This subsection identifies and explores three key settings where cybercriminals converge to meet, communicate, coordinate, commit cybercrimes and conduct "as-a-service" operations, namely: online gaming, hacking forums and dark web markets.

4.4.1 Profiling hackers

The media typically present hackers as malicious criminals and there is a lack of empirical research in the social sciences to refute this popular misconception (Holt, 2020a). However, those within the hacker community or those who define themselves as hackers may engage in hacking for both legitimate and illegitimate reasons, and their motives are nuanced; further empirical research is needed in social sciences to understand the human factors involved in technical crimes (Holt, 2020a). This section will explore what literature does exist in relation to the hacker ethic and hacker subculture, hackers' motives, different types of hackers, and the trade-offs between anonymity and identity for hackers from the perspective of routine activity theory.

4.4.1.1 Origin of the "hacker", hacker ethos and hacker subculture

The origin of hacking is widely recognised to date back to the 1940s at the Massachusetts Institute of Technology (MIT), where students in the model railroad club would alter the electrical systems and equipment of model trains for fun (Holt, 2020a). Early on in the development of computers, the term hacking actually referred to the programmers improving

and maintaining computer systems (Holt, 2020a). The hacker ethos, however, started to form in the early 1960s, during a time in which the use of computer technology became more popular and when there were also significant social movements and social change (Holt, 2020a). The hacker ethos emphasises equal access to computer technology and the knowledge afforded by access to computer technology, a distrust in authority and a recognition that technical skill predominates over any other characteristics indicative of "status" (Holt, 2020a). For example, "phreakers" would hack into phone lines to access paid services for free to disrupt companies who had market control over these services (Holt, 2020a).

During the 1970s there were two innovations in the field: first, the invention of Internet technology and, second, the increased accessibility of computer technology for hobbyists (Holt, 2020a). However, it was not until the 1980s that there was a boom in technology and video gaming, which appealed primarily to younger male populations for entertainment purposes and was targeted at younger populations for education purposes (Holt, 2020a). The formation of hacker communities dates back to the early days of the Internet: hacker "tips" were posted and responded to on bulletin board systems (BBSs), which led to early local hacker groups and eventually national hacker publications (Holt, 2020a). Some hacker communities began to embrace malicious and unethical practices in the late 1980s and 1990s, following the introduction of legislation criminalising hacking, a series of high-profile arrests, increased interest in computer technology from those with lower technical skill and hacker forums for younger hackers (Holt, 2020a). The emergence of the computer security industry saw a divergence in hacker communities, from some viewing hackers in these industries as "selling out" while others viewed this time as the "professionalisation" of hackers (Holt, 2020a).

Since the turn of the millennium, with much of the world moving online, there is a wealth of economic opportunities for hackers, including cybercrime-as-a-service business operations where the skills of hackers are marketed to those with fewer or no technical skill for financial gain (Holt, 2020c). However, the original ethos is still demonstrable in "hacktivism", whereby hacking is used in the name of social and political causes (Holt, 2020a). The modern hacker subculture is an underground community of those who share interest in a deviant act against the norms of a lawful society. The three key values of modern hacker subculture are (Holt, 2020a):

1) the advancement and mastery of technology,

2) status attainment through knowledge and sharing of knowledge, and

3) secrecy or minimising the risk of detection through the use of aliases and covert communications.

4.4.1.2 Hacker motivations

Academic research has explored the typical characteristics or profile of a hacker. Hackers typically start in adolescence and have an affinity for technology. There is limited evidence to suggest that those under 30 tend to hack for malicious purposes, whereas those over 30 tend to hack for legitimate purposes (Holt, 2020a). There is a clear gender gap in relation to hacking: hackers are mostly male, and males are more likely to report engagement in hacking (Holt, 2020a). Technical skill possessed by hackers is likely to be the result of self-directed, rather

than formal education. Contrary to the typical portrayal of a socially isolated young male, hackers are actually typically well connected to like-minded peers through online and offline networks (Holt, 2020a).

One motive for hacking, both legitimate and illegitimate, is thought to be financial gain. Malicious hackers frequently target financial institutions to acquire sensitive data for later sale and profit along with their hacking skills or products on illegal virtual markets (Holt 2020a), whereas ethical hackers profit from their skills and knowledge in the cybersecurity industry as penetration testers or through participation in "bug bounties" (Holt, 2020a). In addition to instrumental motives (i.e., profit), intrinsic motives are thought to be common; hackers may be motivated by various factors simultaneously. Intrinsic motives include entertainment from the thrill, enjoyment of the engagement with technology, amusement, ego, attaining reputation or social status, access to a higher level of hacker strata as well as ideological, political, religious or social causes (Holt, 2020a).

Kirwan and Power (2012, pp. 59-61) review theoretical approaches or explanations of hacker motivation, and there is some agreement across multiple theories. These factors are grouped here into four categories:

- **Intrinsic psychological and emotional drives**, including: curiosity; risk or thrill seeking; addiction; boredom; status attainment; power; ego; group acceptance; entertainment or fun; revenge; self-esteem; catharsis; aggression; frustration; rebelliousness; escapism; control; and malicious or deviant intent.
- **Intrinsic intellectual drives**, including: social engineering or influencing of others; mastery of technology; intellectual or technological curiosity; interest in specific files or information; increasing knowledge or intellectual challenge; success in completion of a hack; and a wish to improve technology or make it safer.
- **Extrinsic social or group drives**, including: group acceptance or peer recognition; notoriety, fame-seeking or media recognition; desire to cause harm to specific targets; peer recognition in hacker subculture; political or social ideology or causes; entrance to certain groups or communities; status or reputation; external pressure from social groups; social disruption; and conforming to perceived gender roles.
- **Financial drives**, including: financial gain; profit; and future career opportunities.

All of these factors can serve to reinforce hacking behaviour.

There is evidence from qualitative studies to support these theories. See Goldsmith and Wall (2019) for an overview of insights from hackers about the "seduction" of hacking. Themes referenced are: thrill, excitement, addiction, curiosity, voyeurism and craftiness. The drivers behind hacking are likely to involve numerous motivations simultaneously. Furthermore, motivational drives may change over time and across different hacking acts (Kirwan & Power 2012).

4.4.1.3 Hacker types and profiles

Hackers can be defined according to three broad categories (Sabillon et al., 2016). The first category is "white hat", or ethical hackers, meaning those who work within the laws while hacking, often as security experts or within the cybersecurity industry. The second category is

"black hat" hackers, meaning those who hack illegally or hack with malicious intent. The third category is "grey hat" hackers, referring to those who are reformed black hat hackers and now work as white hat hackers. With respect to human drivers, these broad groups are likely to subscribe to different ideologies, possess different characteristics and are thought to be driven by different motives.

In terms of the organisation of the hacker community, the sophisticated ("elite") hackers who are capable of accessing most systems and writing sophisticated exploits make up only a small minority (Sabillon et al., 2016). The biggest group are thought to be the least sophisticated hackers ("script kiddies" or "wannabes") and novices, this group generally rely on scripts developed by the elite or more sophisticated hackers to execute attacks. Finally, there are the intermediates (in skill and proportion), who are more advanced than script kiddies and novices, but are not considered part of the elite.

Sabillon et al. (2016, pp. 2-3) present a typology of hacker "classes", summarised in the table below.

Illegal	
Categorised by skill level:	
Elite	Probably gained by a well-known exploit or hack, or by longevity on the scene.
Cracker	This term was created in the early 1990s. It refers to skilled but malicious hackers and differentiates them from the hacker community. They try to take control of systems, and when in danger, will erase any trace of their activities
QPS Hackers	(Quiet, Paranoid, Skilled Hackers) Hacks are carried out mostly out of curiosity, very similar to those of ethical hackers
Virus Writers	Often exploiting weaknesses found by elite hackers and using code methods to execute computer flaws
Wannabe (Lamer)	They want to be hackers and are likely to use "hacker toolkits" without understanding the skills behind them, their actions often result in huge damage
Script Kiddies	The most scorned subgroup, these are the least skilled and youngest members

Categorised by motive or aim:	
Cyber-terrorists	They use stenography and cryptology for exchanging information and sharing plots online, considered among the most serious of computer criminals
Disgruntled (ex) employees	A dangerous and under-publicised group.
Hacktivist	*Name derived from "activism" and "hacking". A very fast-growing hacker subgroup, they are motivated to carry out attacks to satisfy political, religious and social agendas
Cyber-warriors or Mercenaries	An outgrowth of globalisation and the "hacktivism" phenomenon, individuals may be hired to support unlawful operations
Industrial Spy Hackers	These hackers modernised their techniques using information technology to steal intellectual property, inventions and patents, with roots in industrial espionage
Government Agent Hackers	These individuals or groups can work for specific government purposes
Military Hackers	State-sponsored attacks and cyberwarfare. This is a polemic category that was created by the Hackers Profiling Project (HPP) in 2004
Legal	
Ethical Hackers	White-hat hackers who help, for instance by discovering flaws

Table 5: Definitions of different types of hackers (from Sabillon et al., 2016, pp. 2-3)

As shown in this section, there are various different types of hackers. Hackers are differentiated according to the legality of their activity, their skill level and their ideology. Therefore, when considering the human drivers of hackers, it is unlikely that a single motive or driver will apply to this heterogeneous group. Further work is needed to systematically explore what motives apply to large groups (e.g. across multiple different hacker types), specific groups or to specific individuals.

A significant sub population, that requires further study is that of female hackers. Females, relative to males, are much less likely to offend during adolescence particularly in relation to

violent or property offenses. Furthermore, decreased parental guardianship or increased peer interaction are thought to be related to increased offending rate in female adolescents (Daigle, Cullen & Wright, 2007; Holt, Navarro & Clevenger, 2020). This difference is thought to be true of cybercrime also, however there is a lack of quantitative studies specifically investigating differences in perpetration according to gender and what factors may lead to female hacking behaviours. Holt et al. (2020) conducted a recent quantitative study investigating factors that lead to hacking perpetration from both a gender neutral framework and gendered framework to ascertain what factors may be unique to female perpetration of hacking. Holt et al. (2020) found that gender was found to be a significant moderator of hacking, in line with the widely accepted hypothesis that hacking is a male dominated phenomenon. Holt et al. (2020) also found that there are different predictors of female hacking behaviours compared to male hacking behaviours; ownership and use of technology is a significant predictor of male but not female hacking perpetration, whereas peer association and deviant peer behaviours (specifically shoplifting) is a stronger predictor of female hacking perpetration than male hacking perpetration.

4.4.1.4 Routine activity theory: trade-offs between anonymity and notoriety

Routine activity theory is a key criminological theory that, compared to other criminological theories, has been most frequently and successfully applied to cybercrime (see section 4.3.1.3 for a discussion of this theory and its application to cybercriminal motives – also covered in Deliverable 3.1 "Report on drivers of cyber juvenile delinquency"). Cohen and Felson (1979) originally developed routine activity theory. In summary, it was proposed that criminal acts require three convergent pre-conditions: a likely offender, a suitable target, and the absence of capable guardians. Within the context of cybercrime, in a robust study investigating cybercrime victimisation using multivariate analysis (Leukfeldt & Yar, 2016, p. 272) operationalised routine activity theory variables by measuring the following factors:

1. Value – personal financial wealth (income, household income, financial assets etc)
2. Online visibility – level of Internet usage and online activities
3. Digital accessibility – use of operating systems and web browser
4. Personal capable guardianship – technical knowledge and online risk awareness
5. Technical capable guardianship – use of operating system, web browser and virus software

A combination of original and new applications of routine activity theory results in three types of guardianship in relation to cybercriminal offending:

- **Legal capable guardianship** – belief in the likelihood of prosecution, this is unrelated to the cybercriminal(s) and is dependent on the relevant LEA and criminal justice system
- **Technical capable guardianship** – increased technical skill and security/anonymity measures to increase the likelihood of a successful cybercrime attack and simultaneously reduce the likelihood of detection and prosecution
- **Personal capable guardianship** – increased personal control and decreased online risk taking reduces the likelihood of detection and prosecution. However, some level of risk

(decrease in anonymity) must be taken to establish an "identity" within the hacker community

The last two are discussed in relation to three interconnected factors: 1) the proficiency of a hacker; 2) anonymity measures employed by hackers; and 3) identifying hackers online and hacker identities.

Identifying cybercriminals in some instances can depend on their level of proficiency. The likelihood of a hacker's success depends on multiple factors: the hacker's technical mastery, the ability to move through a network, the nature of the attack, the victim's technical mastery, the guardianship of the victim (for example firewalls) and the guardianship of the hacker (Kirwan & Power, 2012).

Anonymity online is also typically determined by the proficiency of the hacker and the steps taken by the hacker(s) to conceal their identity (Pihelgas, 2013). Whilst remaining anonymous online can be for legitimate reasons or to enhance privacy, there are also many ways in which malicious actors increase their anonymity online (Pihelgas, 2013). Complete anonymity online is not possible and there is usually a trade-off; the greater the steps taken to increase anonymity the greater the effort required and the more the associated drawbacks (e.g. loss of ease of use, connection latency and bandwidth) (Pihelgas, 2013). Measures may include: destruction of evidence (log files), identity theft, encryption and well-considered use of personal information (Pihelgas, 2013). Technological tools include proxy servers (see **6.14**), virtual private network servers (VPNs) (see **6.15**), anonymity networks (the onion router, a.k.a. Tor) (see **3.5**) and the use of malware infected zombie computers (Pihelgas, 2013). Concealment of personal information, however, is not a specific technical tool but rather requires careful action by a user, and may be achieved by ensuring they do not reveal website data (e.g. from entering personal data into website fields, logging into social media or making website history available). To conceal personal information a hacker may use a bootable live operating system (from a USB for example) to avoid using the computer's hard disk, or a simpler tactic is the use of "private" web browsers and the deletion of cookies (Pihelgas, 2013).

If a hacker takes the above steps (i.e. skilful use of anonymisation techniques) and does not make any mistakes, it makes it much less likely that attacks can be traced to a source (Pihelgas, 2013). However, there are many ways in which a hacker's identity can be revealed or alluded to online (Pihelgas, 2013). These include the modus operandi, for example the language (e.g. from the code notes) or style of the code used by the hacker, "traces" of tools re-used from previous attacks, the nature of the tools used, the pattern of an attack and the steps taken by the attacker to avoid detection (Pihelgas, 2013).

Alternatively, hackers may choose to sacrifice some level of anonymity for notoriety, i.e. to be "known" within the hacker community. For example, via hacker forums individuals may choose to share "tips", exchange knowledge, trade tools or exploits, or even trade stolen data. Those using such forums will always use an alias or handle to establish an "identity" within the community (Pihelgas, 2013). Other hackers may choose to "sign their work" by implanting their alias or a unique reference within the code (Pihelgas, 2013). Warren and Leitch (2009) identify a type of hacker labelled "hacker-taggers"; hackers who access a system and simply leave a tag without interfering with computer systems or data. These types of hackers are often very competitive, are driven to succeed and share information amongst themselves (Warren & Leitch, 2009). Whilst these hackers, or groups, do not cause damage to computer systems

themselves, they rely on reports of the hack to cause embarrassment or damage to the targets (e.g. politically motivated attacks) (Warren & Leitch, 2009). Kirwan and Power (2012, p. 56) draw connections between "tagging" in hacker subculture and graffiti culture (see references therein).

This review did not identify any research that explicitly explores the trade-offs between skill, anonymity, notoriety and status. However, there seems to be indicative evidence that there is a distinct calculated trade-off between these factors in the hacker community, which is probably dependent on individual factors relating to technical capable guardianship, personal capable guardianship, the nature of the cybercrime, and the individual motives, traits, drives and characteristics of the offender(s).

4.4.2 Profiling malware writers

Some hackers may view themselves as part of a higher social stratum when compared to virus writers; hacking requires a higher level of skill, a higher level of knowledge, and is seen as being "cooler" compared to virus writing, which does not require the same level of skill and can cause indiscriminate harm (Kirwan & Power 2012, p. 73). Though there may be some overlap between hackers and malware writers, it is believed that "there are differences between the methods, motives and skills of the two groups" (Kirwan & Power, 2012, p. 73).

This section will explore what literature does exist in relation to the uses of malware, the motives of malware writers, the characteristics and traits of malware writers, and the motives behind "Malware-as-a-Service" (MaaS).

4.4.2.1 Uses of malware

There are two key components to the use of malware in cybercrime: first, the production or development of the malware itself, and second, the deployment and distribution of malware onto computer systems (Kirwan & Power, 2013). Many forms of cybercrime rely on some form of malicious software (malware), including viruses, worms, adware, ransomware, trojan horses, etc. (Hyslip, 2020). However, the creation of malware itself is not illegal; the use of malware becomes illegal when it is intentionally, and without authorisation, transferred onto a device to cause harm (Hyslip, 2020).

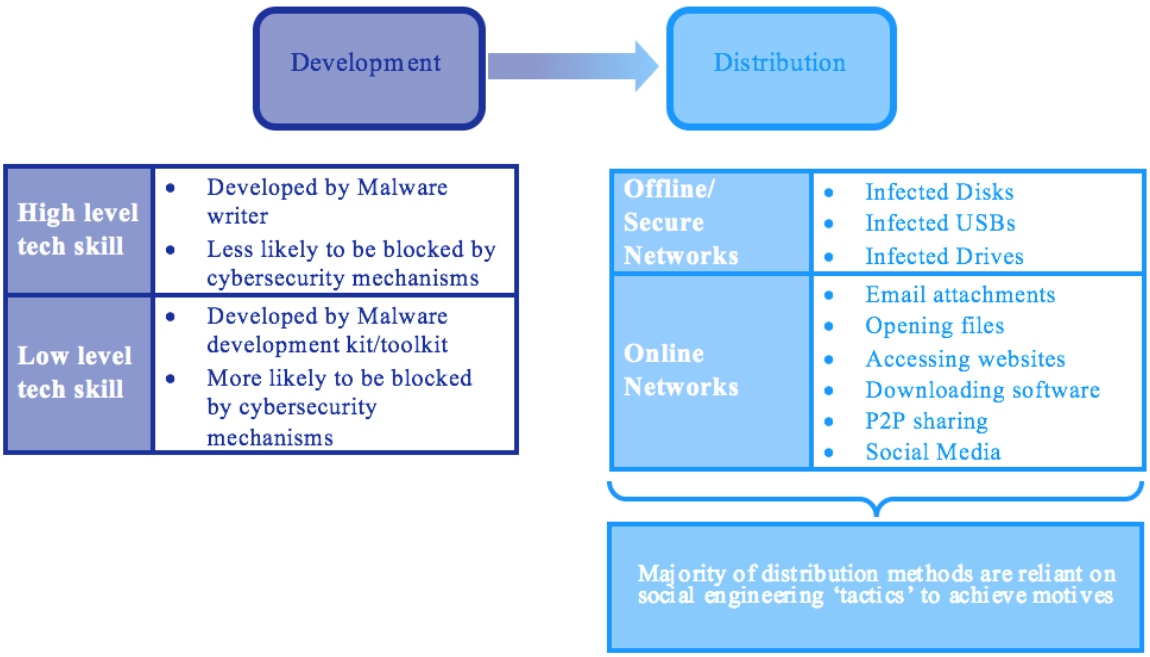


Figure 6: Malware process 'components' summary (Kirwan G. & Power 2012., The Psychology of Cyber Crime: Concepts and Principles, pp. 78-79).

Malware can be used for a variety of different purposes: simply invading the system, but the damage goes no further; damage or corruption to files or data; acquisition of files, data or information; and hijacking of a computer system for other purposes (e.g. creating spam or for use as a "zombie" or "bot") (Kirwan & Power 2012). These different purposes are indicative of the cybercriminal's characteristics and motives.

As with hacking a sub population that requires further academic research surrounds female malware authors. However, there is even less known about female malware writers and the only information found within this review is either speculative or based on a single case study (namely the female coder Gigabyte). Therefore, any findings from these sources should not be used to generalise. This in part may be due to the fact that when virus writers (or more generally hackers) are identified, either none are female, only one of a larger group is found to be female or that females make up a minority of the population of interest (Kirwan & Power, 2013). However, Bocij (2006) suggests that the number of female malware writers may be increasing. The actions of Gigabyte, the only female member of a larger hacker group Metaphase47, is the only case study where the possible motivations of a female virus writer has been examined: Gigabyte famously created malware to humiliate an individual of the cybersecurity industry out of revenge for comments about female virus writers (Kirwan & Power, 2013); is reported to be experimental in virus writing (being the first to write a virus in C# language); similarly to the broader group is thought not to acknowledge the potential harms of malware; and, female virus writers are less interested in payloads[57].

[57] https://www.sciencedirect.com/science/article/pii/S1361372302006097

4.4.2.2 Motives of malware writers

There are theories and indicative evidence that the different components of the malware process, and the "payloads" associated with the malware attack, are reflective of the characteristics, psychology and motives of cybercriminals. In the following sections (**4.4.3** and **4.4.4**), different types of "payloads" are discussed, i.e. the use of malware for financial gain or where malware use is sexually motivated.
Many consider a key motive for malware writers to be financial gain. Malware writers can profit in numerous ways, including illicit means (e.g. extortion, sale of stolen personal information, and through Malware-as-a-Service operations) and legitimate means (e.g. entry into the cybersecurity industry, via antivirus software manufacturers). However, financial gain is thought not to be the primary motive for a malware writer (Kirwan & Power 2012).

Some malware writers do so purely for the intellectual challenge, developing curiosity about how such code works or purely to test their own technical knowledge or skill (Kirwan & Power 2012). They choose not to disseminate their malware, because the dissemination is not needed to fulfil the intellectual challenge, they are fearful of being caught, or it would be a violation of their ethical principles (i.e. they do not wish to cause actual harm) (Kirwan & Power 2012).

However, some do go on to make their code available to others, to attain or increase status within the hacker subculture. Within this group of malware writers, it is thought that some seek the thrill or empowerment associated with their virus being released into the "wild", crave the need for attention and recognition from their peers or the media, or dissociate their action from those who distribute the virus, believing those who disseminate alone may not be culpable for any attack and resulting harm (Kirwan & Power 2012). This final viewpoint may, to a certain extent, be supported by aspects of criminological theory, such as techniques of neutralisation and drift (see section 4.3.1.1). Others who release their code ensure it is known to antivirus companies, to ensure their code cannot be used for illicit purposes, but rather to strengthen computer security (Kirwan & Power 2012). These actions suggest that this group is truly motivated by the intellectual challenge and hacker ethic and have no interest in illicit motives.

The choice of target may also reveal the motivation of a malware writer. For example, some malware writers may be motivated by revenge (e.g. ex-employee or another hacker), by political or social ideology (i.e. to embarrass or gain information about a particular target) or even warfare (i.e. weaponising of malware) (Kirwan & Power 2012).

Other malware writers do so purely for entertainment or out of boredom. This aspect is also seen in many examples of malware, even those believed to be primarily motivated by any of the above reasons, and this is also evident in many sinister forms of malware (Kirwan & Power 2012). Therefore, malware writing can be considered analogous to vandalism, from making themselves known to targets similar to tagging (discussed above in section 4.4) to destruction of their online property (including data files or sensitive information) (Kirwan & Power 2012). Vandalism online may be motivated by similar reasons to real-world vandalism, including entertainment, misplaced aggression or the need to rebel (Kirwan & Power 2012).

4.4.2.3 Characteristics and traits of malware writers

Gordon conducted some preliminary work, although now dated, examining the personality and characteristics of malware writers (Kirwan & Power 2012, pp. 82-85 and references therein).

However, these findings lack generalisability and should be treated with caution, as they are based on a small sample of case studies. Gordon emphasises that virus writers cannot be considered as a homogenised group: rather, the motivation, skill, personality and circumstances are unique to each individual. Gordon also emphasises that it is not legal intervention but the perceived likelihood of prosecution that will deter individuals from virus writing.

Gordon[58] identifies four classes of virus writers, summarised here:

- **Young adolescent** – this group are ethically normal (according to Kohlberg's theory of moral development) and are of either average or above average intelligence. This group were respectful of their parents and demonstrated an understanding of right and wrong, however they also did not accept responsibility for the harmful effects of their viruses. Some younger virus writers will continue into adulthood, but most naturally desist.
- **College student** – this group are also ethically normal and, similarly to their younger counterparts, also did not accept responsibility for the harmful effects of viruses. However, there is limited evidence that, if confronted with the impact of virus writing and forced to address the consequences, virus writers may choose to discontinue their behaviour. Some younger virus writers will continue into adulthood, but most naturally desist.
- **Adult or professional** – this was the smallest group and showed the lowest level of ethical maturity. This group are likely to continue writing and disseminating malware, having continued on past the natural desistance window of "ageing-out".
- **Reformed ex-virus writers** – this group were ethically normal, socially well-adjusted and undecided about the ethical responsibilities associated with virus writing. This group naturally desisted from virus writing because of boredom or a lack of time.

Therefore, from this analysis there are two key groups: youth-limited offenders and persistent lifelong offenders. These two groups are probably very different in their traits, characteristics and ideologies.

4.4.2.4 Motives of 'Malware-as-a-Service' cybercriminals

"Malware-as-Service" (MaaS) mostly involves the distribution of malware, and this is thought to be highly motivated by financial gain. Since malware writing involves a high level of technical skill, early hackers refrained from sharing because of the intense competition and the advantage of using unique malware in the commission of cybercrimes (Hyslip, 2020). However, "as-a-service" business operations allow malware writers to sell exploits on hacker forums, enabling them to profit exponentially and easily from a single piece of malware. Numerous forms of malware are now sold as part of CaaS operations, including banking trojans, keyloggers, rootkits and ransomware (Hyslip, 2020). In addition to the different forms of malware, all forms of malware infrastructure are now also sold through CaaS operations. Malware is only the first step, it must then be delivered and the resulting information must be collected, so both these components are also sold as part of CaaS operations (Hyslip, 2020). Therefore, individuals with virtually no technical ability are able to successfully use malware.

[58] This work is summarised in Kirwan and Power (2012, pp. 82-85), for original references view this text.

This introduces another level of complexity when considering motivations in relation to malware, and raises questions about the motivations of groups or individuals who have no technical ability but are willing to purchase and/or distribute malware. No research identified within this review spoke to the motivation of malware users at this level of granularity.

4.4.3 Profiling ransomware users

There is a particular need to understand the profile of ransomware users; during the Covid-19 pandemic there was a significant increase in the number and impact of ransomware attacks. Cybercriminals during the pandemic initiated more and faster ransomware attacks, were recruiting more collaborators to increase impact, and sold Ransomware-as-as-Service products on the Dark Web (Europol, 2020).

This section will explore what literature does exist in relation to the nature of ransomware and Ransomware-as-a-Service (RaaS), the malicious nature of cyber-dependent crimes (in particular ransomware users), and other forms of cybercrimes where extortion is used for financial gain or other motives.

4.4.3.1 The nature of ransomware and Ransomware-as-a-Service (RaaS)

Ransomware is a type of malware that is used to hold an infected computer to ransom, by encryption rather than theft of information, in order to extort the user into paying a sum in cryptocurrency; a user must either pay the ransom, at which point their data will be decrypted and recovered, or they will probably lose their data, as ransomware encryptions are rarely cracked (see Hyslip, 2020 and references therein). The invention of bitcoin has led to an escalation in ransomware attacks, due to the anonymity that cryptocurrency provides (Hyslip, 2020). The boom in ransomware attacks led to the "Ransomware-as-a-Service" (RaaS)[59] industry. One type of RaaS operation involves the recruitment of others to assist in the spread of ransomware; however, those recruited do not need to have any technical skill, they do not pay for the ransomware, and yet they are paid a portion of the ransom from the RaaS operation, akin to the process of affiliate marketing (Hyslip 2020). Another type of RaaS operation allows for the customisation of a ransomware exploit; however, the customer must set up and maintain the infrastructure to support and run the ransomware (Hyslip, 2020). An example of a widely used RaaS operation is "Philadelphia" ransomware, sold by Rainmaker Labs for $389, this price includes lifetime support and a video for assistance (freely available on YouTube) (Hyslip, 2020).

4.4.3.2 Revisiting the 'malice' in malicious software: dark personality traits and extortionists

Research in this field of malicious software has almost exclusively looked at the malicious nature of technology itself, rather than the malicious intentions of the cybercriminal actor. This is succinctly described in the following quote: "*Most maliciousness cyber research to date has focused on detecting malicious software but fails to analyze an individual's intent to do harm to others by deploying malware or performing malicious attacks… cyber-related maliciousness is neither well-studied nor is it well understood because individuals are not forced to expose*

[59] https://www.europol.europa.eu/newsroom/news/cyber-blue-line-%E2%80%93-new-law-enforcement-frontier

their true selves to others while performing malicious attacks" (King et al., 2018, p. 1). In this section dark personality traits are described and the relation between dark personality traits and (cyber)extortionists.

Dark personality traits or characteristics refers to the collection of personality traits on the negative end of the spectrum of personality traits or characteristics. For example, "The Dark Triad" is a collection of negative personality traits or characteristics that relate to the "everyday" manifestation of three personality disorders: Machiavellianism, psychopathy and narcissism (Selzer & Oelrich, 2021). The Dark Triad has also recently been extended to incorporate traits relating to a fourth personality disorder, namely sadism, and is described as the Dark Tetrad (Buckels et al., 2013). The following is a description of these dark traits (Selzer & Oelrich, 2021, p. 177):

- **Machiavellianism** – marked by a cold, rational and calculative attitude towards human relationships (including manipulation or deception to achieve their goals) and flexible morals
- **Psychopathy** – marked by a disregard for others or callousness (low remorse, empathy or guilt) and consequences (impulsiveness or lack of control), as well as aggression and frequent engagement in anti-social behaviour
- **Narcissism** – marked by lack of empathy for others, need for admiration, and attitudes of superiority or dominance (including grandiosity, entitlement and overinflated sense of confidence) which leads to the manipulation of others
- **Sadism** – marked by "deriving pleasure from inflicting suffering and pain on others" (Althaus & Baumann, 2020, p. 3)

Overall, these four factors show considerable overlap, which suggests the existence of a single underlying commonality, that of human malevolence (Althaus & Baumann, 2020), including tendencies towards "coldness (emotionally), lack of empathy, self-promotion, aggressiveness and unethical tendencies" (Selzer & Oelrich, 2021, p. 177). Dark personality traits are also associated with profit seeking, even at the expense of others (Selzer & Oelrich 2021) and "hard tactics" in the workplace (Jonason et al., 2012). Psychopathy and antisocial traits are strongly associated with criminality (Seigfried-Spellar et al., 2017). Dark personality traits are associated with white-collar crime, theft and deception, and aggression, violence and rape (Selzer & Oelrich 2021). For example, the prevalence of antisocial personality disorder (clinical level of "psychopathy") in criminal populations is more than 10 times higher than in the general population; notably of the criminal sample in this study 45% were convicted of robbery or extortion (Ullrich et al., 2001).

A limited amount of research has investigated dark personality traits within cybercriminal populations. Of the small number of studies that have been conducted, the focus has primarily been cyber-enabled crimes rather than cyber-dependent crimes; psychopathic traits have been found to be associated with cyberaggression, cyberstalking, trolling and digital piracy (Selzer & Oelrich 2021). However, computer deviants do demonstrate exploitive and manipulative behaviours, and narcissistic traits seem to increase the propensity for aggression in hackers (Selzer & Oelrich 2021).

This review identified a single study that evaluated cyber-dependent crime and dark personality traits. This self-report survey, conducted by Seigfried-Spellar, Villacís-Vukadinović and Lynam (2017), found that cybercrime was significantly correlated with other forms of antisocial behaviours (including general, violent and nonviolent antisocial behaviour), and that cybercrime variables (unauthorised access, monitoring network traffic, identity fraud/theft, virus writing) showed the strongest relation to psychopathic variables (Seigfried-Spellar et al., 2017). Of the small sample in the study (N=235), 57% self-reported engaging in hacking (unauthorised access) and 12% self-reported engaging in virus-writing. Hacking and virus-writing were found to be significantly correlated to psychopathic traits (0.31 and 0.36, respectively); in particular, there were significant correlations with sub-scales of antagonism (0.28 and 0.34, respectively), disinhibition (0.25 and 0.29, respectively) and narcissism (0.24 and 0.19, respectively), but no significant correlation with emotional stability.

An exhaustive and comprehensive review might identify a study examining personality traits and the use of ransomware, but it is likely that this type of study has not yet been conducted or has not yet been possible. However, there is anecdotal evidence to suggest that cybercriminals using ransomware may well possess dark personality traits, by their choice of target and actions following a ransomware attack. For example, the healthcare industry is often the target of ransomware attacks. The first known ransomware attack targeted the healthcare industry, and even in the present day the healthcare industry is still the primary target in ransomware attacks (Ferreira, 2018). The WannaCry attack cost thousands of dollars in ransom; however, billions were lost in productivity and health services were severely impacted (e.g. cancelled surgeries, ambulances diverted, and loss of access to patient records) (Ferreira, 2018). More recent examples of callous attacks include a ransomware attack against the Irish healthcare's IT system during the time of a pandemic (Mehta, 2021) and the blackmail of 40,000 therapy patients after a hacker obtained access to their confidential records (Heikkilä & Cerulus, 2020). However, there are examples of hackers and ransomware users showing signs of remorse, which is counter-indicative of dark personality traits, or may indicate that the perpetrators were new to the use of ransomware and not the typical Dark Tetrad personality type that enjoys the suffering of others. Notably, the hackers behind the ransomware attack on the colonial pipeline apologised for the social consequences of the attacks and the impact on the targets of this attack (Clark, 2021).

4.4.3.3 Other forms of extortive acts: sexual violence online

The motivations, characteristics, traits and human drivers of ransomware users may be similar to those associated with other cybercrimes where there is an element of extortion. Demetis (2020) analyses exploitative practices on social media sites. In this qualitative study, 11 broad categories of "dark" social media use emerged (see Demetis, 2020) for a discussion of all 11 categories). Relevant to the topic of this review, "dark" practices online with an extortion element were sexual violence (e.g., revenge porn, sextortion), identity theft or fraud (e.g., catfishing) and extortion in relation to financial gain. For example, "romance fraud"—see Cross (2020) for a more in depth discussion—may be considered a "low tech" version of ransomware; in both instances, the cybercriminal's primary motive is financial gain and, in both instances, the cybercriminal is willing to commit extortion despite the negative consequences to their victim. However, unlike ransomware, **romance fraud** does not require any technical ability: rather, all that is required is to create a fake identity and enter into an online relationship (e.g.,

over social media). These offenders are willing to go to extreme lengths to extort money from their victims under the guise of a romantic relationship. Often victims are financially ruined, psychologically traumatised and, in extreme cases, may attempt suicide (Cross, 2020).

This review did not identify any research looking at the profile of romance fraud scammers. Romance fraud is a relatively new phenomenon and currently the majority of academic research has focussed on understanding victimology and the stages of how this type of crime presents (for example, see Cassandra Cross' work). A review of the literature in relation to romance fraud identified characteristics of victims, who are predominantly female, but in relation to perpetrators found that only one study looked at the profile of the scammers and found that 50 per cent of scams originate from Africa and 16 per cent from Asian and English-speaking countries (Coluccia, et al., 2020).

As with most forms of cybercrime, particularly effective methods evolve into "as-a-service" business models; romance fraud as a business has resulted in the emergence of a new online fraud termed "eWhoring" by offenders (Hutchings & Pastrana, 2019). In this form of fraud, "packets" of sexual media are obtained (voluntarily, through revenge porn or via underground hacker forums) and a fake identity is constructed online. Offenders create opportunities for financial gain by selling said sexual media packets and continue to use tactics to obtain as much payment as possible (some resort to extortion or blackmail, spreading malware via sexual media, scams or attempts to get the victim to pay twice or attempt to target the same victim twice) (Hutchings & Pastrana, 2019). Crucially, those who become involved in eWhoring[60] learn about the process, tips and tactics from hacker forums, including purchasable ebooks and private tuition (Hutchings & Pastrana, 2019). Sexual violence online is often thought of as being a "cyber-enabled" phenomenon; however, in this case, the type of crime is entirely cyber-dependent and is facilitated by the hacking subculture.

There is little research surrounding romance fraud and the newer evolution, eWhoring, particularly the mentality and human drivers of these crimes. However, the callous nature of these crimes is indicative of dark personality traits; these crimes are more personal, are one-to-one attacks. Extreme methods are taken to obtain a financial gain. Victims are often targets of repeat attacks and can be damaged financially, personally and psychologically.

4.4.4 Profiling RAT users

Criminal surveillance manifests in the cyber context through the use of Remote Access Trojans (RATs), a form of malicious code typically disguised as innocuous files to trick users into downloading the malware on their devices. However, some RATters also use social media (e.g. YouTube) and websites to spread RAT malware (Nussbaum & Udoh 2020).

This section will explore what literature does exist in relation to the nature of RAT attacks, the motivation of RAT users, the links between the use of RATs and voyeurism, and the links between RATs and purpose-designed surveillance apps (spyware, stalkerware and creepware).

[60] https://www.urbandictionary.com/define.php?term=eWhoring

4.4.4.1 Nature of RAT attacks

RATs are categorised into four types (see Nussbaum and Udoh 2020, pp. 167-168):

1. Legitimate applications that are produced by known vendors but used for malicious ends
2. Applications written by hackers that can be easily distributed and used by script kiddies or wannabe hackers for stealthy surveillance of victims
3. Applications deliberately written as criminal tools by sophisticated criminal organisations
4. Applications written by nation-states – the most complex, secretive, and stealthy. (Nussbaum & Udoh, 2020, pp. 167-168)

Notable examples of the use of RATs include the Marriott breach and Blackshades RAT. In 2018 an external security analyst discovered a RAT on Marriott hotel systems and determined that the breach had occurred four years earlier. It was estimated at this time that information including "383 million guest records, 18.5 million encrypted passport numbers, 5.25 million unencrypted passport numbers (663,000 from the USA), 9.1 million encrypted payment card numbers, and 385,000 active credit cards" were stolen (Nussbaum and Udoh 2020, p. 164). The data from this type of "loyalty program" breach can be used for various different purposes, including espionage or identity theft, but the information also provides such rich behavioural insights that it could be used to target or influence individuals (Nussbaum & Udoh 2020).

Blackshades is an example of a for-purchase customisable RAT and another example of an "as-a-Service" operation. For a cost of between $40-50, the RAT can be used to log keystrokes, obtain passwords, encrypt files for ransom, activate the webcam and activate the microphone (Nussbaum & Udoh 2020). By 2014, Blackshades RAT had been bought by several thousand individuals, many of them teens, and had been used to infect more than half a million computers in over 100 countries (Nussbaum & Udoh 2020).

4.4.4.2 Motivation of RAT users

RATs are easily acquired and are used for many different purposes, from harassment, to sextortion, to personal gain, to cyberespionage. Therefore, RATs are widely used and are particularly dangerous, as they can be used by individuals with virtually no technical skill but also by the most sophisticated hackers (Nussbaum & Udoh 2020). Young males with an interest in computer technology are believed to be increasingly using RATs to take control of machines (Schell, 2020).

There is some indicative evidence that the primary motive behind the use of RATs is to facilitate deviant sexual drives and sexual violence online. From a case analysis of 132 convictions under the computer misuse act (CMA) in England & Wales, there were four cases where it was explicitly stated that a RAT was used and in all four cases the motive was found to be sexual (Crawford, 2021). For this reason, when a RAT is used for the purposes of sexual violence, it could be considered a gendered criminal behaviour. There is also a clear link between the use of RATs and voyeurism, discussed in the following section.

4.4.4.3 RAT users and voyeurism

Sexual offenses typically fall into two broad categories: contact and non-contact (Kaylor & Jeglic). Voyeurism is a non-contact sexual offense, recognised by the American Psychiatric

Association (APA), and appears in the DSM 5 under paraphilic disorders, where sexual arousal is derived from non-consenting individuals (Kaylor & Jeglic 2021). Voyeurism disorder can manifest as "*sexual gratification on seeing other people perform private activities such as undressing, being naked and/or seeing people performing a sexual act*" (Joseph, n.d.) and, whilst there are a few exceptions, the overwhelming majority of cases involve a non-consenting target (Kaylor & Jeglic 2021). Whilst a diagnosis of voyeurism disorder requires the offender to be an adult (over 18), studies have found that voyeuristic tendencies and behaviours begin earlier, with 50% engaging in voyeurism before the age of 15 (Kaylor & Jeglic 2021). The prevalence of voyeurism is unknown, but there is some evidence that males are much (approximately 3 times) more likely to be perpetrators than females (Kaylor & Jeglic 2021).

A traditional voyeur was known as a "peeping tom", and in earlier eras it would be necessary to go to the victim's location (Kaylor & Jeglic, 2021). However, with the development of technology and the Internet, now a voyeur needs only to connect to the Internet to satisfy the same deviant drives. Some may choose legitimate means, for example there are voyeuristic services and websites offered online for monetary gain (Kaylor & Jeglic, 2021). However, there are also non-legitimate methods such as placing webcams in private locations and streaming to the Internet, or the use of RATs (Kaylor & Jeglic). Offenders using RATs may be unique to other voyeuristic acts online, as these offenders can choose their targets rather than unsuspecting strangers and may have some level of technological skill (Kaylor & Jeglic).

Webcam hacking is a widespread and growing problem, and the technology behind this phenomenon is becoming more complex (for example, concealing the activation of a webcam) making it more likely that unsuspecting victims will be surveilled for longer or may never know they are the victim of a RAT attack.

4.4.4.4 Links to spyware, stalkerware and creepware

Criminal surveillance online is facilitated by the purposeful design of software to facilitate criminal or deviant behaviours relating to sexual violence (typically intimate partner violence) and harassment; this software has been termed spyware, stalkerware or creepware. Software with a legitimate use that is then repurposed for illegitimate reasons (for example, an app designed for parents to monitor their children that is then repurposed to track a romantic partner) is considered spyware (Parsons et al., 2019; Chatterjee et al., 2018). However, there is also a vast industry of stalkerware and creepware apps, that is, software specifically designed for illegitimate purposes, widely available on app stores (see Khoo, Robertson and Deibert (2019) and Roundy et al. (2020) respectively for a discussion of these apps).

Definitions

> Spyware "has a wide range of capabilities, including pervasive monitoring of text and chat messages, recording phone logs, tracking social media posts, logging website visits, activating a GPS system, registering keystrokes, and even activating phones' microphones and cameras, as well as sometimes blocking incoming phone calls"
> (Parsons, et al., 2019, p. 1)
>
> Stalkerware is "commercial spyware applications that can facilitate surveillance of an individual's daily and online activities through their mobile device. When used in the context of intimate partner violence, abuse, or harassment, or gender-based abuse, this technology is referred to as stalkerware. Such software grants an operator unauthorized remote access to a device and often compromises it without the knowledge or consent of the device owner, the targeted individual. On this basis, stalkerware may be considered a form of malware, against which digital devices and personal data must be secured."
>
> (Khoo, Robertson, & Deibert, 2019, p. 4)
>
> Creepware is "apps whose primary use … is enabling non-expert users to mount interpersonal attacks."
> (Roundy, et al., 2020, p. 626)

Based on the definitions above, these types of apps represent the commercialisation of RAT malware (or malware generally) and are now widely available to those with little or no technological ability; this software can be used for a variety of deviant or illegitimate purposes or to satisfy a range of motives. This review did not identify any literature that speaks to the motives of the software developers. The software, on the other hand, is purposefully designed to perpetuate sexual violence and interpersonal violence online. Therefore, the motivation behind the user of these apps is somewhat obvious; however, it is uncertain, particularly as no research was identified that explored the mentality (e.g. moral reasoning, traits, characteristics or personality) behind the downloading and use of such apps. Overall, when considering the human drivers behind criminal surveillance online, motives relating to sexual and interpersonal violence and abuse need to be considered in future research, particularly if this is the primary motive when the barrier of technological ability is lowered (i.e. by "as-a-Service" operations, or through purposely designed software in the form of commercial apps).

4.4.5 Online offender convergence settings

Offender convergence settings traditionally were physical locations, such as cafes or bars, where criminals would meet and expand their criminal network (Leukfeldt et al., 2017). However, the Internet provides specific offender convergence settings for cybercriminals. Younger populations in particular are driven to communicate with peers or associate with like-minded communities and overall, these communities are considered to be a potent factor in the commission and facilitation of cybercrime. Cybercriminals converge in online settings to meet, communicate, coordinate, commit cybercrimes and conduct "as-a-Service" operations. Felson coined the term "offender convergence settings" to describe certain physical locations, e.g. local tough bars, in which (potential) offenders meet each other. Here they relax with friends and acquaintances, meet new people, exchange information, sell stolen material or plan new criminal acts. The perpetrators of cybercrime also make use of such locations, albeit digitally in so-called "virtual forums" (Soudijn & Zegers 2012, p.111). In this section, three key examples of online offender convergence settings are explored: namely online gaming, hacker forums, and Dark Web markets.

4.4.5.1 Gaming as a gateway

When investigating cyber-dependent cybercrimes, there is a focus on the development of technological skill and tools required to commit such crimes but less of an understanding as to why motivations change over time and how accompanying attitudes that encourage involvement in cyber-dependent type cybercrimes develop or change over time (Goldsmith & Wall, 2019). One explanation is that skills *and* attitudes are "honed" over time through participation in activities such as online gaming (Goldsmith & Wall, 2019). Within gaming "cheats" are widely accepted and used, players that use cheats are perceived to display mastery and obtain status, which positively reinforces the use of cheats and the associated rewards, much like hacking (Goldsmith & Wall, 2019).

Using hacker testimony, Wall (2017) determined a four-stage model by which gamers are gradually seduced into cyberdeviance and cybercrime:

1. From fair use of video games to using cheats in order to win
2. From use of gaming cheats to use of hacking and gaming forums to learn how disable a friends' computer in order to win
3. From learning how to disable a friends' computer to more extreme hacking tactics (e.g. DDoS)
4. From more minor forms of offending to more extreme forms of hacking offenses (e.g. large DDoS attacks or use of ransomware)

This pathway is supported by LEA findings (Goldsmith & Wall 2019) and by empirical research (for example, see Pastrana et al., 2018, as discussed in section 4.4.5.2). Although gaming itself is not dangerous on its own, it is almost always a common link for those who do progress to criminal activities online (Goldsmith & Wall 2019). Within hacking, peer influence plays a critical role in encouraging criminal activity and in minimising the negative connotations; hacking activity is often viewed by hackers as positive deviance even if not strictly legal (Goldsmith & Wall 2019).

4.4.5.2 Hacking forums and hacker recruitment

Forums are the medium most commonly used by cybercriminal communities to communicate (Huang et al., 2018): "underground forums allow criminals to interact, exchange knowledge, and trade in products and services. They also provide a pathway into cybercrime, tempting the curious to join those already motivated to obtain easy money" (Pastrana et al., 2018, p. 1845). Online forums are used by cybercriminals and cyberdeviants to communicate, exchange knowledge and trade in illicit materials or services, for example, financial fraud and trading of personal data, eWhoring (discussed above), or trading of virtual game items (see Pastrana et al., 2018, and references therein). There is a vast amount of literature investigating the dynamics of these forums and criminal activity. However, there is a paucity of research investigating the motivations, interests beyond fraudulent activities, and timelines ("pathways") of those who use the forums (Pastrana et al., 2018).

This review identifies four key studies that have accessed and analysed hacking forums. Three use CrimeBB (database of posts from a number of hacking forums: see the table below, collected by Cambridge Cybercrime Centre[61]) and one obtained leaked data from Darkode, an invitation-only hacker forum.

Forum	Language	Members	Threads	Posts	Oldest
Hackforums	EN	573,925	3,856,143	40,196,641	01/2007
Kernelmode	EN	1,441	3,144	25,024	03/2010
Offensive Community	EN	10,593	18,436	58,779	06/2012
Multiplayer Game Hacking	EN	452,186	739,527	8,907,938	12/2005
Stresserforums	EN	764	708	7,069	04/2017
Greysee	EN	440	1,239	6,969	06/2015
Garage4Hackers	EN	872	2,096	7,697	07/2010
SafeSkyHacks	EN	7,378	12,892	26,842	03/2013
Antichat	RU	77,865	242,408	2,449,221	05/2002
RaidForums	EN	43,278	33,100	124,776	03/2015

Table 6: Forums and forum information in the Crime BB dataset. Source: Akyazi et al. (2021, p. 4)

Firstly, findings are discussed in relation to the CrimeBB data set. Recent research has sought to categorise and quantify CaaS activity on these forums (see Akyazi et al., 2021, for a discussion of CaaS on Hackforums) and to build machine learning classification models to identify post "type" and intent of the author from their use of language (see Caines et al., 2018, for a discussion of this model). Important findings from these studies are that "*more than half of the cybercrime trade is dealt with privately via messaging apps and private messages on the forums* (Akyazi et al., 2021, p. 11) and machine learning models can soon be used to predict

[61] https://www.cambridgecybercrime.uk/datasets.html

and analyse forum user interactions and behaviour, which can be extrapolated across other forums (Caines et al., 2018).

However, only one project was identified that used the CrimeBB dataset to specifically focus on the motivations and interests of the forum users. Pastrana et al. (2018) used a tool (CrimeBot) to scrape online forums, to include more recent posts from hacking forums, focussing on cybercriminal communities. The authors collated interests according to seven categories and observed that "*many members start with interest in hacking, gaming or technology, but these interests move to market and money-making forums once they start exchanging currencies*" (p. 1853). Furthermore, within these online communities non-malicious interests (e.g. gaming and technology) coexist with malicious interests (e.g. black-hat hacking and illicit currencies). Thus Pastrana et al. (2018) hypothesise that those with non-malicious interests may become enticed by "easy money-making methods" or wish to gain a reputation or status within this community, after being exposed to these interests and activities within the forum. This is also supported by Wall's four-stage model (2017), discussed above (in section 4.4.5.1).

Secondly, findings are discussed from a study that analysed posts in the invitation-only forum Darkode. Another type of forum used by the hacking community are invitation-only forums, often used by the most skilled and successful cybercriminal hackers (Dupont et al., 2017). Dupont et al. (2017) analysed the Darkode forum's communications leaked by a white-hat hacker under the alias "Xylitol", which contained 4 years of communications between the world's most advanced and prolific hackers, after a member of Darkode starting using the same alias ("Xylitol") to conduct cybercriminal business online. This research focussed on the selection process of 344 new members of the forum; therefore, the focus of this research is more on the dynamics of the forum. However, as this consists of open access data,[62] it can be further examined to conduct a similar analysis to that of Pastrana et al. (2018), to look for initial interests and pathways over time to explore the motivations and characteristics of cybercriminal offenders.

Another key aspect to consider in relation to motives and interests is that they are exemplified by the "human resources" aspect of hacker forums (Huang et al., 2018). Huang et al. (2018) identify "Hacker Training as a Service (HTaaS)" which provides how-to guides and online schools that help someone to become a proficient or qualified hacker within the community; there are also similar legitimate programs within the cybersecurity industry. Future research could aim to examine the tactics and modus operandi of offenders who are looking to train or recruit novice hackers, and what this may tell us about cybercriminal motivations and psychology. Huang et al. (2018) also identify "Hacker Recruiting as a Service (HRaaS)", whereby cybercriminals actively recruit others to carry out an attack. Their choice of accomplices may provide an indication of their motives: for example, state-sponsored cyber-attacks may involve the recruitment of non-affiliated hackers to reduce culpability and political risks (Huang et al., 2018).

4.4.5.3 Dark Web markets

The anonymity and global nature of the Internet has allowed the proliferation of illicit online markets on the Dark Web (Liggett et al., 2020). The four major markets are drugs, firearms,

[62] This dataset can be downloaded here: http://darkode.cybercrime-tracker.net

cybercrime goods and services, and child sexual abuse material (CSAM). The nature of these markets is summarised in this section (see Liggett et al., 2020, for a more in-depth discussion and references therein):

- **Drug markets** – online drug markets are rapidly increasing. The most infamous and largest (although only accounting for a small percentage of all illegal drug trade) was Silk Road, until it was dismantled in 2013. However, others have filled the void (e.g. Silk Road 2.0, the Cannabis Road, Agora, Pandora and Evolution). Online drug sales are facilitated by the use of cryptocurrency, anonymous delivery (e.g. through the post), the perception of safer interactions, more reliable "products" through rating systems, greater accessibility to wider networks, international trade, and ways to avoid or minimise punishment.
- **Firearm markets** – the Dark Web allows for regulatory loopholes in the sale of firearms (particularly for those who are unable to obtain firearms through legitimate means) coupled with the anonymity and ease of access that the Dark Web provides. However, very little is known about how these markets operate, or how many firearms are bought and sold on these markets. One study estimated 136 firearm transactions per month across 60 firearm markets, with the US being the primary supplier of firearms for illegal marketplaces. Individuals can purchase anything from military grade weapons to explosives; the most common products are pistols, rifles and submachine guns. Again, cryptocurrency is often used (with bitcoin being the primary currency) and prices of firearms are often inflated (compared to offline illicit firearm markets).
- **Cybercrime: "Cybercrime-as-a-Service" (CaaS) markets** – the skills of hackers ("cybercrime consulting"), cybercrime tools, stolen data (typically financial information and personal data) and malware are forms of for-profit cybercrime "products", and have therefore been made available on both open and Dark Web markets. Through these markets, those of especially high technological expertise (sellers) enable those with low expertise (buyers) to carry out sophisticated hacks (under the Crime-as-a-Service model).
- **Child sexual abuse markets** – online sex markets form a spectrum from legal to deviant to illegal. Anonymised access (e.g., use of Tor) has facilitated the distribution of child sexual abuse material (CSAM) and online child sex trafficking. Such markets involve numerous forms of child sexual exploitation, including the acquisition of CSAM, production of CSAM, distribution of CSAM, and real-world sexual abuse of children (resulting in significant physical and psychological trauma). Disturbingly, such activity online is pervasive: NCMEC's CyberTipline has received 43 million reports of child sexual exploitation. As part of LEA investigation, INTERPOL holds a database of more than 1 million images of CSAM. Individual markets have been found with more than 200,000 members; and, whilst only two per cent of the Dark Web markets are child sexual abuse markets, these sites account for 80 per cent of Tor traffic. Unlike the previous three markets, the "products" in these CSAM markets are transferred for free, the majority of CSAM is transferred using P2P networks or via Dark Web subcultures where the more severe forms of CSAM are transmitted. Over recent years, with the advent of smartphones, webcams, social media and apps, the nature of CSAM has changed: children are often groomed, coerced or extorted into creating self-generated CSAM, which now accounts for most of the CSAM found on the open and

Dark Web. A small number of CSA markets (between 7.5-18%) are commercial and profit from the sexual abuse of children in numerous ways, ranging from payment for livestream of CSA, payment for individual materials or memberships, advertising of CSA sites, sex trafficking and cybersex tourism.

- As shown in the above descriptions drawn from Liggett et al., 2020, the motives of the users of these markets are financial gain, procurement of illicit items and engagement in deviant or illicit activity. However, we found no research that looks at the profiles of Dark Web market users.

4.4.5.4 Social media & cyber- dependent crime

McGuire (2019) produced a report summarising the uses of social media in relation to cyber-dependent cybercrimes. As the uses of social media in cybercriminal activity is significantly under researched, the findings of this report are summarised in this section.

The report notes that social media platforms can provide a source of direct revenue, believed to be approx. $3.25 billion annually, and these sources may include sale of illegal pharmaceutical drugs, sales of stolen data, fraud, crypto mining malware, and romance fraud. However, there are many other ways that social media can be used by cybercriminals for financial gain, illegal drug sales, sale of 'fake' products (including fake PPE), or sale of hacking products or services. Additionally, social media platforms are one of the main sources of malware infections for both individuals and organisations. Social media platforms provide many means of deploying malware, as these platforms may include images, videos, adverts and plug-ins. Social media are also successful for deploying malware, as users are likely to be more trusting and click on links and the phenomenon of 'chain exploitation', which comprises three key elements; amplification, persuasion and contagion. Amplification refers to the sphere of influence on social media, as many people now use social media as a source of information and news, and information can proliferate rapidly and widely though social media networks. For instance, news, including fake news, spreads rapidly and limitlessly via social media platforms, technical devices, forums and websites (Aiken, Farr & Witschi 2021) illustrating individual's readiness to trust links shared on social media blindly, and how vulnerable the public are to spreading fake news or information or dangerous links online. Persuasion refers to the ability of cybercriminals to successfully engage victims and then persuade users to interact with content, for example click on links or download content, or persuade users to engage in a desired behaviour, for example voting choices or money muling. Social media research has found that frequent social medias are more susceptible to persuasion tactics than less frequent users. Contagion refers the ability of materials to 'go viral' via social media.

Aside from social media platforms being a vehicle for cybercriminal activity, social media platforms themselves and more importantly the personal data they collect are an attractive target to cybercriminals, it is believed that up to 50% of the data being traded online could have been obtained through social media breaches, that social media attacks have increased significantly in recent years and social media is an effective gateway to target businesses (when users log in to social media accounts in the workplace). Furthermore, cybercriminals are able to tailor their attacks to the site being used. For example, phishing is widely used on Facebook (and is considered to be a primary target), YouTube is a popular vehicle for pushing links in relation

to popular content that leads to a malware download, and via Instagram credential stealing apps cybercriminals are able to send out spam ads from accounts related to the stolen data.

McGuire (2019) identifies the criminal threats or 'services' (known as CaaS) commonly found on social media in relation to cyber-dependent crimes:

- Digital currency and cryptocurrency scams
- Cryptojacking and cryptomining malware
- Buying through fake likes to boost malicious profiles
- Trade or sharing of exploits
- Botnets or booter hire
- Hacking services (readily found on up to 40% of social media sites)
- Trade of stolen data
- Alternatively, the trade of stolen data is used a lure to deploy malware

McGuire (2019) identifies criminal activities commonly found on social media in relation to cyber- enabled crimes:

- Money laundering via social media (known as money muling) is rapidly increasing and teenagers are thought to be a key demographic (as young as 14)
- Sale of illegal drugs on the surface web (via social media platforms)
- Fraudulent brand/product pages are used to send out spam or distribute malware
- Dating scams or romance fraud
- Violent behaviour, for example incitement of violence or gang recruitment
- Identification of sites shown on social media to burglarise

4.5 Conclusion

This chapter sought to explore the human factors of cybercrime, underpinned by distinctive aims. The first aim of this chapter was to give a broad overview of the academic literature exploring human drivers of technical (Type 1) cybercrimes, by identifying key academic theories in relation to disciplines: criminology, psychology, cyberpsychology and neuroscience. This holistic, multidisciplinary approach to a better understanding of the human factors behind cybercrime was presented in sections 4.2-4.4 of this chapter. The second aim was to explore recent empirical studies relating to profiling and motivations relevant to a select sample of Type 1 cybercrimes, and this was presented within section 4.4 of this chapter. A non-exhaustive literature review was carried out, and more than 140 references were included. Some concluding points have been summarised below:

- This chapter highlights the significance of applying (and adapting) classical theory and techniques originating within the disciplines of criminology, psychology, forensic psychology and neuroscience to the context of cybercrime and cyberdelinquency.
- Understanding the human, as well as the technical factors behind cybercrime is vital.

- The constantly evolving, far reaching and anonymous world of cyberspace poses an array of obstacles in the endeavour to better understand cybercrime and cyberdelinquency.
- The Covid-19 pandemic has led to unprecedented volumes of online audiences. In turn, the world has witnessed surges in cybercrime worldwide, with trends as reported in section 4.2.3. While there is little literature available to investigate the malicious and callous underpinnings of profiting financially from a global pandemic, this chapter has attempted to touch on some of these questions, specifically relating to the human factors of cybercrime perpetration.
- Section 4.4 of this chapter highlights the diversity of cybercriminals, especially in relation to motive, but also their characteristics.
- Section 4.4 provided a multitude of recent examples of cybercrime found in the literature. It highlighted how particular human factors (such as hacker's signature) might actually lead to identification and prosecution by LEAs.
- This chapter further highlights the complexities of approaches to profiling cybercriminals, which may be largely dependent on the crime itself, or the level of skill involved, the ethos of virtual subcultures and, of course, the multitude of human factors that are at play.

In conclusion, the human factors of cybercrime are complex and nuanced, yet are crucial to grasp. The use of a multidisciplinary approach is key. For the most part, motivations can be largely dependent on the crime itself, whereby understanding risk factors and environmental influences can help to reduce cybercriminality. While some theories included in this chapter (such as Deterrence Theory and Labelling Theory) have been applied and adapted more recently in the content of cybercrime, both theoretically and in the design of primary and secondary data analysis, there are still multiple calls for more research that seeks to further explore the human factors of cybercrime and cyberdelinquency. Collaborative research that both applies and adapts relevant existing multidisciplinary theories, and that attempts to explore youth cognitive processes and motivations behind harmful online behaviours, must be implemented if cybercrime is to be tackled efficiently via targeted prevention and intervention initiatives.

5 Techniques, tactics and tools of cybercriminals

5.1 HACKING AND DUAL-USE TOOLS 98
5.1.1 Nmap 98
5.1.2 Metasploit - penetration testing 99
5.1.3 John the Ripper/ THC Hydra 99
5.1.4 Burp Suite 100
5.1.5 OWASP ZAP 100
5.1.6 Nessus 100
5.1.7 Tcpdump/Wireshark 100
5.1.8 sqlmap 101
5.1.9 Kali Linux 101
5.1.10 Aircrack-ng/Kismet 101
5.1.11 Nikto 101
5.1.12 PowerShell 101
5.2 MALWARE 103
5.2.1 Malware 103
5.2.2 Trojans 104
5.2.2.1 Infostealers 104
5.2.2.1.1 Lokibot 104
5.2.2.1.2 Formbook 105
5.2.2.1.3 Raccoon 105
5.2.2.2 Backdoors, Remote Access/Administration Trojans (RATs) 105
5.2.2.2.1 Remcos 106
5.2.2.2.2 Ave Maria/Warzone 106
5.2.2.2.3 Agent Tesla 106
5.2.2.2.4 njRAT 107
5.2.2.2.5 Andromeda 108
5.2.2.2.6 Zegost 108
5.2.2.2.7 Poison Ivy 108
5.2.2.2.8 IRCBot 109
5.2.2.2.9 Gh0stRAT 109
5.2.2.3 Trojan Bankers 109
5.2.2.3.1 TrickBot 109
5.2.2.3.2 Qakbot 111
5.2.2.3.3 Emotet 112
5.2.2.3.4 Ursnif (Gozi) 113
5.2.2.3.5 Neverquest 113
5.2.2.3.6 Dridex 114
5.2.2.3.7 Zbot (Zeus) 114
5.2.2.3.8 Fareit 114
5.2.2.3.9 Dyre 115
5.2.2.4 Rootkits 116
5.2.2.4.1 Sality 116
5.2.2.4.2 Alman 116
5.2.2.4.3 Necurs 117
5.2.2.4.4 Rustock 117
5.2.2.4.5 ZeroAccess 117
5.2.2.4.6 Sinowal (the Bootkit) 117
5.2.2.4.7 TDSS 118
5.2.2.5 Keyloggers 118
5.2.2.5.1 Phoenix keylogger 118
5.2.2.5.2 Ardamax 119
5.2.2.5.3 HawkEye 119

5.2.2.5.4 iSpy ... 119
5.2.2.6 Ransomware ... 119
5.2.2.6.1 WannaCry ... 120
5.2.2.6.2 Petya/NotPetya ... 121
5.2.2.6.3 Ryuk/Conti ... 122
5.2.2.6.4 CryptoLocker/CryptoWall/TorrentLocker ... 123
5.2.2.6.5 Dharma/CrySIS ... 123
5.2.2.6.6 DoppelPaymer/BitPaymer/Grief ... 124
5.2.2.6.7 Maze/Egregor/Sekhmet ... 124
5.2.2.6.8 REvil/Sodinokibi/GandCrab ... 125
5.2.2.6.9 RagnarLocker ... 126
5.2.2.6.10 Darkside ... 126
5.2.2.6.11 Lockbit ... 127
5.2.2.6.12 SunCrypt ... 128
5.2.2.6.13 Avaddon ... 128
5.2.2.7 Exploit kits ... 129
5.2.2.7.1 Blackhole Exploit kit ... 129
5.2.2.7.2 Angler Exploit Kit ... 132
5.2.2.7.3 Neutrino Exploit Kit ... 134
5.2.2.7.4 Nuclear Exploit Kit ... 136
5.2.2.7.5 Fallout Exploit kit ... 138
5.2.2.7.6 Magnitude Exploit Kit ... 138
5.2.2.7.7 RIG exploit kit ... 140
5.2.2.8 Botnets ... 142
5.3 EXPLOITATION ... 144
5.3.1 Trends in Exploitation ... 144
5.3.1.1 Major events ... 144
5.3.1.1.1 2000 - ILOVEYOU worm ... 144
5.3.1.1.2 2003 - SQL Slammer ... 145
5.3.1.1.3 2010 - Stuxnet ... 145
5.3.1.1.4 2010 - Blackhole EK ... 146
5.3.1.1.5 2012 - Flashback OSX ... 146
5.3.1.1.6 2012 - Flame ... 147
5.3.1.1.7 2013 - Angler EK ... 147
5.3.1.1.8 2014 - Heartbleed, Shellshock ... 147
5.3.1.1.9 2017 - CCleaner supply chain ... 148
5.3.1.1.10 2017 - Wannacry ... 148
5.3.1.1.11 2017 - NotPetya ... 148
5.3.1.1.12 2017 - Coinhive ... 149
5.3.1.1.13 2017 - Emotet MaaS ... 149
5.3.1.1.14 2020 - Solarwinds supply chain ... 150
5.3.1.1.15 2021 - Microsoft Exchange Server hack ... 150
5.3.1.2 Top exploited vulnerabilities 2016-19 ... 150
5.3.2 Acquisition of exploits ... 152
5.3.3 Summary and the future of exploitation ... 152
5.4 EMERGING ATTACKS ON IOT AND CPS ... 154
5.5 USE OF WEBSITES AND HOSTING SERVICES ... 155
5.6 SOCIAL ENGINEERING, USE OF 'HUMAN' VULNERABILITIES ... 157
5.6.1 Influence on the choices of cybercriminals ... 159
5.6.2 Influence on technical and business strategies ... 159
5.7 SUPPLY CHAIN ATTACKS ... 160
5.8 ATTACKS ON CLOUD PLATFORMS ... 168
5.8.1 Malware delivery ... 168
5.8.2 Cloud as a phishing platform ... 168
5.8.3 Account compromise ... 169
5.8.4 Misconfiguration abuse ... 169
5.8.5 Resource hijacking in the cloud ... 170

5.9 ATTACKS ON COLLABORATION PLATFORMS AND TOOLS 170
5.10 CYBERSTALKING 172
5.11 IDENTITY THEFT - THEFT OF BANK CARDS 174
5.12 DRUG CRIME 175
5.13 HUMAN TRAFFICKING 177
5.14 CSAM 178
5.14.1 How is CSAM distributed online? 178
5.14.2 Where is CSAM located? 179
5.14.3 Business model 179
5.15 ONLINE HARASSMENT - CYBERBULLYING 180
5.16 EXTORTION – SEXTORTION 181
5.17 GROOMING 182
5.18 REVENGE PORN 183
5.19 HATE SPEECH 184
5.20 CYBER TERRORISM – VIOLENT EXTREMISM - RADICALISATION 185
5.21 THE GENDER DIMENSION 186
5.21.1 Perpetrators 187
5.21.2 Victims 188
5.22 THE GEOGRAPHICAL DIMENSION OF CYBERCRIME 189
5.22.1 Russia ex Soviet Union 190
5.22.2 Nigeria 192
5.22.3 China 193
5.22.4 South America 193
5.22.5 India 195
5.23 THE AGE DIMENSION OF CYBERCRIME 197
5.23.1 Perpetrators 197
5.23.2 Victims 198

Software built mainly for legitimate security purposes, such as network management and monitoring, vulnerability assessment, penetration testing, etc., remains a staple for cybercriminals. With support from developers and the community, most of these tools have become powerful through time. Unfortunately, they can be misused to provide ease in performing malicious activities and gain a foothold on the cybercriminals' targets.

Attacks utilising applications built into operating systems have become more and more prevalent. Living-off-the-land attacks ensure that the attack will run successfully, since the applications used are natively supported. In addition, they can evade traditional protection mechanisms, as the misused applications are not black-listed by default. A popular example is PowerShell. Some common use cases for PowerShell are to download and execute additional payloads and gain information on the target system that can be used for lateral movement.

Malware has evolved through the decades. From simple viruses, worms and trojans, malware has now combined various functionalities to increase the chances of attacks hitting their targets, commonly financial gain or stealing sensitive information. In the past decade, ransomware has become prolific. As the name suggests, it encrypts files in a system, which in effect prevents users from accessing them, and holds the decryption key for ransom. In recent years, ransomware gangs have become bolder and have started to take on high-value targets such as

big private organisations and public offices or agencies, where one successful attack can lead to a huge payout of up to millions of dollars. Many organisations have become more aware of this threat and have learned to add extra safety measures. Now, they have a choice not to pay the ransom and just recover their files from backups. Cybercriminals quickly reacted and used another extortion approach, which is threatening their victims with the leakage of sensitive stolen information.

One might wonder how ransomware attacks became more sophisticated and successful. To answer the question, one must look into the malware ecosystem. Cybercriminals started to specialise, and malware-as-a-service was offered to other cybercriminals. A good example is Emotet[63], which is notorious for having a huge botnet that can easily spread other malware such as ransomware. Some individuals behind Emotet were apprehended in January 2021, which disrupted their operations. However, other groups—such as the one behind Trickbot[64], which is also running its operations since 2016—are starting to fill the gap left behind by Emotet.

Exploit kits are a collection of software tools that exploit different vulnerabilities, usually of web browsers and their plugins and components. They are commonly used to perform drive-by downloads, which initiate the download of malware such as ransomware without the user's knowledge. They were prominent between 2013-2015, before organisations such as Google, Microsoft and Apple took action to address the common vulnerabilities. Authorities also started tracking down the threat actors behind the exploit kits, which caused a further drop in their activities. Nevertheless, there are still some exploit kits that are still active even today.

In recent years, some high-profile breaches have been associated with supply-chain attacks, which insert malicious code into components of software or services such as utility software, managed service providers, and code repositories, etc. Some attacks even replace the updaters of this software, which will instead execute malicious code or download additional malware. Organisations often trust these kinds of software, as they are known to be legitimate, and only carry out minimal auditing, if any, before using them. This trust enables cybercriminals to fly under the radar for a long time and bide their time to do reconnaissance before they carry out their plans and secure their targets.

As individuals and organisations adapt new technologies, more attack surfaces are introduced. The most recent examples are IoT, Cloud and Collaboration platforms. In the IoT space, the most notorious threat is Mirai, which was able to infect millions of vulnerable IoT devices and use them to mount large-scale distributed denial-of-service (DDoS) attacks to take down websites and servers. IP cameras are also being targeted, which could allow attackers to spy on video feeds. Some of these IoT devices were not designed with security in mind, and patching the vulnerabilities for some of them is not straightforward.

Organisations started migrating their assets to the cloud. Along with all the benefits, this entails more of the same threats, such as misuse to deliver malware, phishing, account compromise, misconfiguration abuse and resource hijacking. As Covid-19 arrived, remote work, classes and events have become the norm and the use of collaboration platforms has become a must. As one would expect, cybercriminals adapted to this new trend and started targeting collaboration platforms. Examples of attacks are meeting bombing, where attackers can join the meetings

[63] https://en.wikipedia.org/wiki/Emotet
[64] https://en.wikipedia.org/wiki/Trickbot

uninvited, and exploitation of vulnerabilities, which can lead to download of malware, hosting of malware, phishing, account compromise and impersonation.

In this section we present the specific tools, techniques and tactics used by cybercriminals today.

5.1 Hacking and dual-use tools

Tools intended for research and educational purposes are often abused by hackers to conduct malicious operations and launch attacks. There is a thin line that separates such security tools from being categorised as hacking tools. In this section we make a reference to dual-use tools. Such tools were not initially created for malicious purposes, but the wide spectrum of security functionalities they provide make them ideal for use by cybercriminals.

5.1.1 Nmap

Nmap (Network Mapper),[65] is probably the most popular network scanner. It is an extremely feature-rich program, it is free to use and open-source. Nmap is mainly used to discover services and hosts in a network. Nmap does not enable a graphical user interface in its basic version. A graphical interface can be installed additionally with the Zenmap framework.

Nmap is designed to quickly scan large networks, although it works very well against single host targets. Its main goal is to discover the software they run and the services provided, including the active and open ports where both legitimate and malicious users can connect.

Nmap operates by sending specially crafted raw packets to the target and analysing the responses. Unlike many simple port scanners, which only send packets at a predefined constant rate, Nmap monitors network conditions (latency fluctuations, network congestion, scanning intervention) during its execution and adjusts its settings accordingly.

Its main features include:

- Host discovery – determines which hosts are available on the network
- Port scanning – identifies what services these hosts offer and which ports are opened, accepting connections
- Software version detection – detects various applications and their versions, e.g. firewalls in use.
- OS detection – detects the underlying operating system of the hosts and hardware specifications of existing network devices
- Scripting engine – allows users to extend its functionality by writing scripts using the Lua scripting language

While Nmap is commonly used for auditing and security checking, many system and network administrators also find it useful for routine tasks such as network inventory, managing service upgrades, monitoring hosts or services for downtime and measuring the network response time.

[65] https://nmap.org/

Moreover, due to the large and active user community that provides feedback and contributes to its functionality, Nmap has been able to extend its core features and discovery capabilities even further. Nmap is enabled with a scripting engine (NSE) that can transform it into a powerful vulnerability scanner. Two of the most popular scripts, nmap-vulners and vulscan, enable the tool to produce Common Vulnerabilities and Exposures (CVE) information from a remote or local host. This scanning mode enables the user to detect the presence of known software vulnerabilities in network services.

Cybercriminals use the Nmap tool mainly in the initial phases of their attack to perform network reconnaissance (network services and vulnerabilities discovery).[66]

5.1.2 Metasploit - penetration testing

Metasploit[67] can be considered as a dual-use tool. This tool has been widely used for penetration testing and digital forensics by cybersecurity experts since its creation in 2003. Metasploit is a very powerful open-source tool that comes with a variety of ready to run solutions, while it can be easily customised and modified according to the needs of any user.

Metasploit can be used by security engineers to probe a network for vulnerabilities and to perform an ethical penetration test on a system to discover any underlying weaknesses. However, at the same time, a cybercriminal can use it in a similar manner to exploit its results and eventually compromise the target. Once the discovery and analysis stage has been completed and the tool has discovered any vulnerabilities that exist, then a cybercriminal would be ready to enter the exploitation phase. Metasploit comes with more than 1600 different exploits and more than 300 different payloads ready to be used with a few clicks. Custom payloads can also be used for successful exploitation of the target. Moreover, Metasploit provides plenty of other post-exploitation capabilities that can be used by digital forensics investigators, such as memory dumping, deleted file recovery, registry and storage analysis and much more. Similarly, these functionalities could be the object of criminal acts.

5.1.3 John the Ripper/ THC Hydra

John the Ripper[68] (JRR) is an open-source password security auditing and password recovery tool available for all the popular platforms. It supports hundreds of encrypted password formats and uses brute-force and dictionary methods to crack a password. JRR has been widely used by security staff and administrators to spot weak passwords and weak password policies. However, at the same time, cybercriminals could use such tools to penetrate a system by cracking an access password. Once the tool succeeds in cracking the password, an attacker could gain full access to the system and move into the next phase of their attack.

Another popular password cracking tool is THC Hydra.[69] This tool attempts to gain access to a system remotely. THC Hydra supports more than fifty protocols and operates over the network. In the same context as John the Ripper, this tool enables researchers and security consultants to

[66] https://blog.teamascend.com/cyberattack-game-plan-how-attackers-choose-their-targets-and-plan-their-attack
[67] https://www.metasploit.com/
[68] https://www.openwall.com/john/
[69] https://github.com/vanhauser-thc/thc-hydra

discover how easy it would be to gain unauthorised access to a remote system. However, cybercriminals could misuse this tool for their malicious operations.

5.1.4 Burp Suite

Burp Suite[70] is a popular platform for performing security tests on web applications. One of its main features is to intercept and modify the HTTP communication between a browser and a web application. In this way the user can manually test the security of the application and discover vulnerabilities.

Other features include a spider (a web crawler that detects and maps all the pages that make up the target web application), an intruder (a tool that performs automated attacks on the target web application to discover vulnerabilities: e.g. XSS, SQL injection, parameter manipulation), and a repeater (a tool that replays requests and performs stress tests)

5.1.5 OWASP ZAP

OWASP ZAP[71] (short for Zed Attack Proxy) an open-source web application security scanner maintained under the umbrella of the Open Web Application Security Project (OWASP). This tool has a variety of security functionalities that can be leveraged by professional security engineers but also by cybercriminals. ZAP operates as a proxy monitor between a browser and a web application by intercepting all the communication messages being exchanged. The operator is able to inspect the messages, modify the contents if needed and detect any vulnerabilities in the application. Other features of the platform include an automated scanner, brute-force scanner, port scanner, spider and a fuzzing mechanism.

5.1.6 Nessus

Nessus[72] is a popular proprietary remote security scanning tool, which scans a system against thousands of known vulnerabilities and alerts the user if it discovers any weaknesses or misconfigurations. This tool is used by administrators for prevention purposes but also by cybercriminals to gain access and harm a system by exploiting the tool's results.

5.1.7 Tcpdump/Wireshark

Tcpdump[73] and Wireshark[74] are open-source tools that are widely used for capturing and analysing network traffic. Available on almost all platforms, these tools enable administrators to troubleshoot network issues and security engineers to perform deep packet inspection, by actively or passively monitoring a network, for research and educational purposes. However, these tools should be used on a network only if there is explicit authorisation for monitoring. Consequently, such tools could be also used by a cybercriminal for eavesdropping.

[70] https://portswigger.net/burp
[71] https://www.zaproxy.org/
[72] https://www.tenable.com/products/nessus
[73] https://www.tcpdump.org/
[74] https://www.wireshark.org/

5.1.8 sqlmap

sqlmap[75] is an open-source penetration testing tool used for detecting and exploiting SQL injection flaws. This tool can be used to discover SQL vulnerabilities that affect any application that uses an SQL database. sqlmap operates on all popular database systems and fully supports six SQL injection techniques: Boolean-based blind, time-based blind, error-based, UNION query, stacked queries and out-of-band.

5.1.9 Kali Linux

Kali Linux[76] is an operating system, based on a Debian-derived Linux distribution, that was specially designed for digital forensics and penetration testing. Kali is freely available and is very easy to modify or customise as it is an open-source platform. Additionally, most of the tools that we have described above, along with hundreds of other security tools, are pre-installed in Kali Linux. This makes Kali Linux an ideal platform for both ethical hacking and criminal operations.

5.1.10 Aircrack-ng/Kismet

Aircrack-ng[77] and Kismet[78] specialise in the analysis of wireless traffic. Aircrack-ng is a software suite that can sniff and analyse 802.11a, 802.11b and 802.11g traffic. It includes a packet sniffer, a WEP and WPA/WPA2-PSK cracker, a packet injector and several other tools for 802.11 wireless LANs. Kismet is a network detector, packet sniffer, and intrusion detection system for 802.11 wireless LANs, similar to Aircrack-ng. Its engine can sniff 802.11a, 802.11b, 802.11g, and 802.11n traffic. Kismet also includes wireless intrusion detection (WIDS) features, such as detecting active wireless sniffing programs, as well as a number of wireless network attacks.

5.1.11 Nikto

Nikto[79] is a free program that is used to scan web servers for vulnerabilities. Nikto can detect over 6700 potentially dangerous files/CGIs, checking for outdated versions of over 1250 servers and version-specific problems on over 270 servers. It also checks for server configuration items, such as the presence of multiple index files and HTTP server options.[80]

5.1.12 PowerShell

PowerShell is a Windows built-in modern command shell, a command-line tool to interact with the operating system.

[75] https://sqlmap.org/
[76] https://www.kali.org/
[77] https://www.aircrack-ng.org/
[78] https://www.kismetwireless.net/
[79] https://cirt.net/Nikto2
[80] https://en.wikipedia.org/wiki/Nikto_(vulnerability_scanner)

Although originally built with powerful features to manage windows-based endpoints and servers, PowerShell has become one of the most popular attack tools among cybercriminals.

One of the multiple benefits of PowerShell is the fact that it can be found natively on Windows-based operating systems and attackers do not need to introduce compiled malware into the environment. This effectively reduces the detection opportunities for the victim. PowerShell provides a wide range of functions to interact with the operating system, remote operating systems and the active directory domain, all of which are often necessary steps in breaches against organisations—for example by more advanced ransomware groups.

Additionally, PowerShell as a scripting language provides attackers with the possibility to build and automate attack tools. Naturally the flexibility and power provided by PowerShell is attractive to cybercriminals.

Several different attack tools have been developed over time with PowerShell, and a large portion of these are considered "red team" tools, developed and provided publicly for lawful security testing of organisations.

According to interviews with the F-Secure Detection & Response team (DRT), in the vast majority of the breaches by low- to mid-tier cybercriminals, PowerShell is used as a tool. Some of the most commonly observed PowerShell security testing tools & frameworks include but are not limited to:

- PowerSploit modules
    - "PowerSploit is a collection of Microsoft PowerShell modules that can be used to aid penetration testers during all phases of an assessment." [81]
- PowerShell Empire framework
    - "Empire is a post-exploitation framework that includes a pure-PowerShell2.0 Windows agent, and a pure Python 2.6/2.7 Linux/OS X agent. It is the merge of the previous PowerShell Empire and Python EmPyre projects. The framework offers cryptologically-secure communications and a flexible architecture. On the PowerShell side, Empire implements the ability to run PowerShell agents without needing powershell.exe, rapidly deployable post-exploitation modules ranging from key loggers to Mimikatz, and adaptable communications to evade network detection, all wrapped up in a usability-focused framework. PowerShell Empire premiered at BSidesLV in 2015 and Python EmPyre premeiered at HackMiami 2016." [82]

In addition to dedicated attack tools built on PowerShell, it is often used in other stages of a breach. Some other common use cases for PowerShell in cybercrime:

- Powershell as a dropper
    - A dropper is often used as one of the first payloads to deliver another piece of malware/executable. PowerShell can be used to implement typical dropper capabilities, such as embedding a payload, decryption/decoding of the payload, obfuscation of own code, execution of the embedded payload, writing the payload to disk and scheduling execution. A common occurrence of PowerShell in email-based campaigns is inside .lnk files in which a shortcut (.lnk) is

[81] https://github.com/PowerShellMafia/PowerSploit
[82] https://github.com/EmpireProject/Empire

modified in a way to execute a malicious PowerShell command instead of a file on disk.

- Powershell as a downloader aka “download cradle”
  - One of the most common use cases of PowerShell among cybercriminals is the so-called downloader, which is a piece of code similar to a dropper, but built to download the second-stage payload from a remote location instead of embedding it. A downloader written in PowerShell can be a very small piece of code and very straightforward.
- PowerShell for local and network discovery
  - PowerShell as an interactive shell is often used to execute other native binaries in order to collect information from the localhost, or from other hosts in the network. Often, sub-phases in an attack killchain can be automated with PowerShell scripts where such network/host discovery takes place and results are automatically staged.

5.2 Malware

5.2.1 Malware

Malware is an abbreviation for **mal**icious soft**ware**: software that is designed to harm computer systems and data. There are many malware categories so far, and many more will be generated in the future. Researchers have attached different names to each malware instance and have classified malware into families and taxonomies that share similar properties, behaviour and targets.

Historically, the terms “computer virus”, “worm” and “trojan” came up during the 70s, in science fiction stories and novels. The following decade, the first computer viruses and worms attacked systems around the world. Since then, numerous terms have been used to identify the types of malware that have evolved, but the terms virus and worm still dominate the press and the public discourse.

A virus is a type of malware that is attached to other programs, files or scripts and stays dormant until they are activated. After the virus gets executed, it replicates itself and infects other files and programs of the system. Viruses usually spread through shared files, email attachments and malicious websites. The term virus is widely used by the media and regular end-users for any type of malware and has been confused with worms and trojans.[83,84]

Worms are another major category of malware that, in contrast to viruses, are standalone and do not need a triggering event in order to run. Worms are found in email messages, shared files, network shares, hidden in network packets and in messages of modern messaging apps. After the initial infection, they exploit security vulnerabilities on targets and use the network to replicate and propagate themselves across multiple systems. Thus, each infected machine will scan and infect other machines in the same network. Worms are known for their ability to infect large numbers of computers rapidly.

[83] https://www.csoonline.com/article/2615925/security-your-quick-guide-to-malware-types.html
[84] https://www.comtact.co.uk/blog/what-are-the-different-types-of-malware/

Today, most malware is a combination of traditional malicious programs, often including parts of worms, viruses and trojans, a kind of malware that we describe in detail in the following section. Malware has evolved over the last years and plays a key role in the cybercrime ecosystem. For each different type, we describe its attributes and how it is used to facilitate cybercrime operations. Additionally, we list the most popular instances of each type, based on how frequently they have appeared in recent cases of cybercrime.

5.2.2 Trojans

Trojans borrowed their name from the story of the Trojan War and the wooden horse that the Greeks used to enter the city of Troy and finally win the war. A trojan is a type of malware which masquerades itself as legitimate software and appears to be benign, but secretly performs malicious actions that could harm the user's system, data or privacy. Trojans are generally spread by some form of social engineering. Unlike viruses and worms, trojans generally do not attempt to infect other files or otherwise propagate themselves through the network to other systems. Trojans evade detection by having dormant capabilities, hiding components in other files, forming part of a rootkit, or using heavy obfuscation.

Many different payloads of trojans create many subcategories and variations of malware that encrypt files (ransomware), provide remote and unauthorised access (backdoors, rootkits, RATs), harvest the device (botnets), steal bank credentials (trojan-banker), steal sensitive information (infostealers), download other harmful programs (trojan-downloader), and more.

5.2.2.1 Infostealers

Infostealers[85] are a type of malware that collects sensitive and private information from the system that has been infected. This information is often related to user credentials but also includes any financial and personal data available.

5.2.2.1.1 Lokibot

LokiBot[86] was first reported in 2015 and it is still very popular among cyber criminals. It has been used to steal cryptocurrency wallets (CryptoCoin wallets) and credentials by enabling a keylogger that monitors browser and desktop activity. LokiBot also installs a backdoor into the system in order to be able to fetch additional malware. The malware usually targets Windows and Android operating systems and is distributed via spam emails, malicious websites and messages from instant messaging apps.[87]

Lately, Trend Micro researchers discovered a new LokiBot campaign that targeted the installer of the Epic Games store, the development company behind popular games such as Fortnite (Trend Micro, 2020). This variation of the malware introduced an unusual installation routine in order to avoid the detection mechanisms of antivirus systems. Upon execution, the malware installer drops two files and eventually gets the trojan running on the system.

[85] https://blog.f-secure.com/what-are-infostealers/
[86] https://us-cert.cisa.gov/ncas/alerts/aa20-266a
[87] https://www.zdnet.com/article/new-lokibot-trojan-malware-campaign-comes-disguised-as-a-popular-game-launcher/

5.2.2.1.2 Formbook

Formbook monitors activity on the Firefox web browser in order to steal login details for the Facebook social media network. When the user logins to Facebook through Firefox, the trojan steals any data the user enters into the login page and forwards them to its C&C server.

It can also capture screenshots, remove user cookies, disable task manager and download additional malware. The trojan is spread as a specially-crafted document file attached to spam email messages.[88]

5.2.2.1.3 Raccoon

Raccoon was first seen in the wild in April 2019. It is another popular infostealer trojan that is capable of recording the user's activity in the browser (cookies, history, autofill) and stealing login credentials and cryptocurrency wallets. It is sold in underground markets, as an instance of Cybercrime-as-a-Service and Malware-as-a-Service, with a price that ranges from $75 US per week to $200 US per month.[89] Delivery methods for the victim include exploit kits and phishing campaigns.[90]

5.2.2.2 Backdoors, Remote Access/Administration Trojans (RATs)

A backdoor is any type of software that gets installed in a compromised computer system in order to allow unauthorised access to it. Backdoors can be installed in both software and hardware components. From there, they may be used to install more malware on the computer or to gain access to credentials, sensitive data and information about available networks, services and other workstations. In some cases, worms—another type of malware—are designed to take advantage of any backdoors that may be present on the system from a previous attack. For example, the Code Red[91] worm establishes a backdoor that has been used by other worms, such as the Nimda[92] worm, to spread.

Backdoors have evolved in recent years and, according to a 2020 report from Malwarebytes (MalwareBytes Labs, 2020), they were the fourth most common threat detection for businesses, with an increase of 14% over the past year.

Backdoors have a strong presence in cybercrime operations. They are widely sold in illegal marketplaces, either as standalone applications or as part of more complex malware applications. Some of the most popular backdoors are discussed in this section (Trend Micro, 2016b).

RATs are malicious programs that allow an attacker to control a victim's system remotely and execute commands. RATs essentially act as backdoors, but may also contain infostealer and keylogger elements.

[88] https://www.f-secure.com/v-descs/trojan_agent_formbook.shtml
[89] https://blog.trendmicro.com/trendlabs-security-intelligence/raccoon-stealers-abuse-of-google-cloud-services-and-multiple-delivery-techniques/
[90] https://www.cyberark.com/resources/threat-research-blog/raccoon-the-story-of-a-typical-infostealer
[91] https://en.wikipedia.org/wiki/Code_Red_(computer_worm)
[92] https://en.wikipedia.org/wiki/Nimda

5.2.2.2.1 Remcos

Remcos emerged in 2016, being peddled as a service in hacking forums, and was later advertised, sold, and offered cracked on various sites and forums.[93] Remcos typically targets the Windows OS and embeds a specially-crafted settings file into an Office document, thus allowing the attacker to run malicious code without any further warning or notification.[94] In 2017, it was being delivered via a malicious PowerPoint slideshow, but it recently made its way to phishing emails.

After a successful infection, Remcos gives full control over the system and enables the attacker to run keyloggers and surveillance applications. By issuing commands, the criminal can delete files, download additional malware with backdoor capabilities and control it, get the output of the keylogger, capture the screen and steal cryptocurrency wallets, user credentials and sensitive information.

5.2.2.2.2 Ave Maria/Warzone

Ave Maria, also called Warzone RAT, was first seen towards the end of 2018. The malware is available under subscription in underground marketplaces and arrives on the victim's system mainly as a result of phishing mails.[95] Ave Maria is capable of stealing a wide range of data from infected machines. Even such well-protected information as credentials stored in Mozilla Firefox are not safe, despite the PK11 encryption used. Since its discovery, many variations have emerged and have been discovered by researchers.[96]

5.2.2.2.3 Agent Tesla

Agent Tesla is another popular password stealer trojan that has been around since 2014.[97] It was sold as legitimate software through an official website that provided monthly subscriptions with different configurations such as Bronze, Silver, Gold and Platinum, each providing different levels of capabilities and customer service. While the official creator stated that the Agent Tesla software should only be used to monitor the buyer's personal computer, they provided instructions through the official website on how to best exploit vulnerabilities and avoid antivirus software.

The malware was created using the .NET framework and aimed to steal personal information from web browsers, email clients and FTP servers and send it back to its C&C server (SMTP or FTP).[98] Agent Tesla was supplied with a dedicated builder that had a user friendly control panel; thus, for example, it could enable even a non-technical attacker to pack the payload into a malicious document. After 2015, an updated version of the malware and its control panel allowed the attacker to automatically capture snapshots and remotely activate the webcam on the victim's computer. The malware was equipped with multiple mechanisms in order to avoid antivirus detection and for that reason it was able to turn off Windows processes to remain hidden.

[93] https://www.trendmicro.com/en_us/research/19/h/analysis-new-remcos-rat-arrives-via-phishing-email.html
[94] https://blog.malwarebytes.com/detections/trojan-remcos/
[95] https://any.run/malware-trends/avemaria
[96] https://malpedia.caad.fkie.fraunhofer.de/details/win.ave_maria
[97] https://www.reliaquest.com/blog/malware-analysis-what-is-agent-tesla-and-how-can-you-protect-your-enterprise-from-it/
[98] https://any.run/malware-trends/agenttesla

Agent Tesla has exploited the COVID-19 pandemic and featured in more attacks in the first half of 2020 compared to the TrickBot and Emotet malware, according to SentinelOne's SentinelLabs.[99] New variants have been introduced with enhanced functionality, and the malware has been widely used in Coronavirus-themed phishing campaigns and in the latest targeted campaigns against the oil and gas industry.[100]

5.2.2.2.4 njRAT

njRAT[101], otherwise known as Bladabindi, is a widely used RAT that was first detected back in 2013. It is available on the market, it has several implemented evading techniques and features an abundance of online tutorials and information for users.[102] It was used in targeted attacks against the Middle East in the year 2014. It was created by a hacking group with the name Sparclyheason.

njRAT's main features include activation of the webcam and microphone, stealing passwords, keylogging, termination of processes, manipulation of files, execution of processes and many more. njRAT also has trojan banker capabilities and is known for grabbing bitcoins and targeting cryptocurrency wallets stored in the infected machines. Some distribution methods include the Discord app, which was used as part of spam campaigns, and through fake updates for Adobe products from malicious websites.

In July 2014, the Computer Emergency Response Team-India (CERT-In) reported that a clandestine multi-identity virus was spreading through removable USB flash drives, including other malware.[103] A typical variant of this trojan propagated by dropping a copy of itself on to removable drives and creating a shortcut file with a folder icon and name of the drive.

In 2016, several spam campaigns spreading the njRAT trojan targeted the servers of Discord, a free VoIP chat service very popular among gamers.[104] The attackers' motive was to use njRAT to steal in-game currency or gear by gaining access to gaming-related accounts and sell them on the dark market.[105] The attackers either join channels and leave links as messages, leading to malicious downloads of njRAT, or create Discord servers and invite users to join their channels.[106]

In 2017, criminals targeted a website of Islamic State in order to distribute the njRAT trojan. Anyone visiting the website encountered a prompt for a fake Flash update. The exploited website hosted a file simply named "FlashPlayer_x86.exe" that was disguised as the Flash installer and actually was a dropper (a piece of software that installs malware) for njRAT.

[99] https://labs.sentinelone.com/agent-tesla-old-rat-uses-new-tricks-to-stay-on-top/
[100] https://threatpost.com/oil-and-gas-agent-tesla-spyware/154973/
[101] https://www.microsoft.com/en-us/wdsi/threats/malware-encyclopedia-description?name=MSIL/Bladabindi
[102] https://any.run/malware-trends/njRAT
[103] https://www.firstpost.com/tech/news-analysis/hacking-virus-bladabindi-targets-windows-users-in-india-steals-personal-info-cert-in-3654589.html
[104] https://news.softpedia.com/news/gaming-voip-servers-abused-to-spread-remote-access-trojans-rats-509496.shtml
[105] https://news.softpedia.com/news/online-gaming-currencies-used-to-launder-money-for-cyber-criminals-509177.shtml
[106] https://www.symantec.com/connect/blogs/attackers-use-discord-voip-chat-servers-host-nanocore-njrat-spyrat

5.2.2.2.5 Andromeda

The Andromeda backdoor is a window bot that can communicate with C&C servers and execute commands. It has a modular architecture and its capabilities can be extended. There are many variants of this backdoor, which make up the Andromeda family of backdoors.

Usually, they are used to load other malicious applications on to the infected computer system. ANDROM accounts for 44% of the backdoors that are used in cybercrime (Trend Micro, 2016b).

5.2.2.2.6 Zegost

Zegost, also known as Zusy/Kris, is a remote access trojan that can allow an attacker to take control of the victim's machine. It has been around since approximately 2011 and was believed to be derived from Gh0stRAT (another well-known RAT). It's primary goal is to steal information and spy on intended victims by having capabilities that include logging keystrokes, collecting video footage from webcam, identifying RDP port numbers, QQ login number, and uploading/executing follow-up payload.[107]

Historically, Zegost has been attributed to Chinese cybercriminals. It is also known for its craftiness in delivering targeted attacks, including detection evasion and persistence. One of its attacks involved compromising a Chinese real-estate and shopping site by injecting a malicious script that redirected users to a server that leveraged an Adobe Flash vulnerability (CVE-2015-5119) leaked from the Hacking Team, an offensive security company that provided tools to law enforcement and government agencies in 2015.[108]

Zegost was also used in a targeted attack to two sites of government agencies in Nepal, the National Information Technology Centre and the Office of the Prime Minister and Council Minister, in 2012. The threat actors injected malicious code that exploited a Java vulnerability (CVE-2012-0507) to install the Zegost backdoor.[109]

5.2.2.2.7 Poison Ivy

Poison Ivy is a publicly available RAT that was first released in 2005. It was notable for being part of sophisticated and high-profile targeted APT attacks in the years after it was released. In 2011, attackers used it to compromise RSA's SecurID infrastructure and steal data about its SecurID authentication system. The threat actors behind the attack were linked to Chinese cyber criminals. The attack was carried out by exploiting a zero-day vulnerability. Another notable campaign in which PoisonIvy was involved was known as Nitro, and targeted chemical manufacturers, government agencies, defence contractors and human rights groups.[110]

Variants of it can be created by a builder kit that allows an attacker to build and customise their own Poison Ivy server. Its features may have different spying functionalities, such as logging keystrokes, capturing screens, recording audio or webcam footage, and accessing passwords and password hashes.[111]

[107] https://blog.talosintelligence.com/2021/04/threat-roundup-0416-0423.html
[108] https://www.zscaler.com/blogs/security-research/chinese-backdoor-zegost-delivered-hacking-team-exploit
[109] https://threatpost.com/nepalese-government-sites-hacked-serving-zegost-malware-080812/76893/
[110] https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-poison-ivy.pdf
[111] https://www.f-secure.com/v-descs/backdoor_w32_poisonivy.shtml

5.2.2.2.8 IRCBot

An IRCbot is a type of backdoor that connects to an Internet Relay Chat (IRC) server and waits for commands to execute from a remote attacker. The bot is controlled via messages sent to it. Different variants of IRCbot were found to exploit several vulnerabilities to spread itself, such examples are as the following:

- Windows Server Service (MS06-040)[112]
- Microsoft LSASS Service (MS04-011)[113]
- Microsoft ASN.1 library (MS04-007) ports 80, 139, 445
- Microsoft Workstation Service WKSSVC (MS03-049) port 135
- Symantec Antivirus and Client Security vulnerability ports 2967, 2968

Several tasks can be performed by an attacker, some of which may include starting an FTP server, performing a ping, SYN, ICMP and UDP flooding, collecting system information, redirecting traffic, stealing CD keys for popular games, downloading and executing files, logging keystrokes, scanning and exploiting vulnerable computers.[114]

5.2.2.2.9 Gh0stRAT

Gh0stRAT is an open-source RAT that has been used by cybercriminals in various targeted attacks against government and military targets, as well as high-profile cyberespionage operations against the Dalai Lama's computer network. It is known as part of the Gh0stNet operation, a cyber espionage network whose command & control servers reside in China and which started in 2009. Its features mainly aim to steal and spy on targets by logging keystrokes, stealing credentials, capturing microphone and webcam, and many more. It was also known to be used in Operation Aurora, a series of cyberespionage attacks attributed to the Chinese APT (advanced persistent threats) group with ties to the People's Liberation Army. The attack was aimed at many organisations, including Google, Adobe and other large companies.[115]

Since its source code is publicly available, there have been different variants of Gh0stRAT, which is used in many APT attacks. One example was the attack against Amnesty International, whose websites in the UK and Hong Kong were compromised to serve a variant of Gh0stRAT[116].

5.2.2.3 Trojan Bankers

A specific type of trojans that focus on stealing money from the victim by using a variety of techniques, such as stealing credentials, intercepting online banking sessions and grabbing cryptocurrency wallets.

5.2.2.3.1 TrickBot

TrickBot is a very popular trojan that has been very active over recent years. The first version of TrickBot, which is also known as Trickster or TrickLoader, appeared in 2016 and initially

[112] https://www.f-secure.com/v-descs/ircbot_st.shtml
[113] https://www.f-secure.com/v-descs/backdoor_w32_ircbot_bnz.shtml
[114] https://www.f-secure.com/v-descs/backdoor_w32_ircbot_bns.shtml
[115] https://threatpost.com/new-backdoor-ddos-malware-co-existing-gh0strat-infected-machines-110612/77191/
[116] https://www.zdnet.com/article/amnesty-websites-compromised-in-gh0st-rat-attack/

targeted the corporate networks of banks in US, Australia and Canada, but quickly expanded its focus on banks in Germany and other financial institutions. It is considered to be a successor to the Dyre (Dyreza) malware, which was active until 2015 and reportedly stole millions of US dollars from the Ryanair airline, among others.[117]

TrickBot mainly spreads through spam campaigns. Once a host is infected, TrickBot also exploits vulnerabilities in the SMB protocol to infect even more hosts in the local network of the organisation. Exploiting SMB enables malware to quickly propagate throughout an organisation where hardware and software configurations tend to be fairly homogeneous.[118]

TrickBot can also send spam emails itself to increase spreading. In some cases, these messages are sent from trusted addresses within the organisation. Experts believe that TrickBot may have compromised more than 250 million email accounts so far.[119]

TrickBot's functionality has evolved since its appearance and now encompasses multiple uses.[120] It can spy on other information to gain access to email accounts, system and network information and tax information. It can install a backdoor on your system so that it can be accessed remotely and used as a part of a botnet. It acts as a malware dropper and installs additional malware, such as the Ryuk ransomware.

Bleeping Computer has tracked the evolution of TrickBot and its attacks from its start as a trojan banker until today:[121]

- June 2017: Attacks on PayPal accounts and business CRMs.
- July 2017: Added support for a self-spreading component
- September 2017: Added support for stealing funds stored in Coinbase.com accounts
- March 2018: Added a screenlocker component
- October 2018: Adopted DKIM to bypass email filters
- November 2018: Started stealing Windows problem history
- January 2019: Partnership with Ryuk ransomware
- February 2019: Upgraded to grab credentials used to authenticate to remote servers using VNC, PuTTY, and Remote Desktop Protocol (RDP)
- July 2019: Added a separate module for stealing browser cookies,
- July 2019: New distribution method through fake Office 365 sites
- July 2019: New version that prevents its detection and removal by Windows Defender
- August 2019: Stealing PIN codes from Verizon Wireless, T-Mobile and Sprint users

[117] https://www.computerweekly.com/news/4500245366/Ryanair-remains-tight-lipped-over-33m-hacker-theft
[118]https://www.forbes.com/sites/leemathews/2019/07/14/stealthy-trickbot-malware-has-compromised-250-million-email-accounts-and-is-still-going-strong/
[119]https://www.forbes.com/sites/leemathews/2019/07/14/stealthy-trickbot-malware-has-compromised-250-million-email-accounts-and-is-still-going-strong/
[120] https://blog.f-secure.com/what-is-TrickBot/
[121] https://www.bleepingcomputer.com/tag/TrickBot/

- November 2019: Added a password grabber module that could be used to steal OpenSSH private keys and OpenVPN passwords and configuration files
- December 2019: A malicious campaign baited targets with phishing techniques, abusing Google Suite cloud services to infect them
- December 2019: Lazarus group of hackers use TrickBot
- January 2020: Added a UAC bypass targeting the Windows 10 operating system
- March 2020: Ryuk ransomware attacked Epiq Global via TrickBot infection
- March 2020: A new COVID-19 spam campaign targeted people in Italy
- March 2020: Used a malicious Android application (TrickMo) to bypass two-factor authentication (2FA) protection used by various banks
- April 2020: Developers of TrickBot introduced BazarBackdoor, a new stealthy backdoor
- July 2020: Started to check the screen resolutions of victims to detect whether the malware is running on a virtual machine
- July 2020: Once again TrickBot comes hand in hand with Emotet spam trojan.
- September 2020: US hospitals were attacked by Ryuk ransomware, which got installed by TrickBot instances that allegedly were spread during Emotet campaigns.

From the end of September 2020 the TrickBot botnet was focused on by the US government and several security companies and providers. Multiple disruptive actions were performed in a coordinated effort to take down the botnet. An undisclosed number of command & control servers were also taken down to cut their communication with the bots at hosting provider level. The botnet used its fallback mechanisms and managed to recover. Reportedly, as of October 2020, the Ryuk ransomware seeded through TrickBot is still infecting computers across the world.

5.2.2.3.2 Qakbot

QakBot[122], also known as Qbot or PinkSlip, is a banking trojan that was first spotted in 2007. Like other modern multifaceted trojans, QakBot has greatly evolved and currently presents worm capabilities and can be used as a keylogger, as a backdoor and also as a dropper. Another sophisticated feature it includes is a polymorphism mechanism that allows the malware to self-mutate in transit, as it moves inside a company's network.[123]

QakBot has been distributed through a few highly-targeted campaigns aimed only at large banking and financial companies. A recent phishing campaign (March 2019) spread QakBot with the help of delivery emails camouflaged as parts of previous conversations. The phishing email included a link to a dropper script, packaged as a ZIP archive, capable of installing QakBot after being launched by the victim. Recent cases include QakBot campaigns that targeted customers of 36 different U.S. financial institutions, as well as two banks in Canada and the Netherlands.[124] Even the Emotet botnet started to push the QakBot trojan at an

[122] https://securelist.com/qakbot-technical-analysis/103931/
[123] https://www.bleepingcomputer.com/tag/QAKBOT/
[124] https://www.f5.com/labs/articles/threat-intelligence/qbot-banking-trojan-still-up-to-its-old-tricks

unusually high rate, replacing the longstanding TrickBot payload. Recent news is that QakBot is using a new template for its distribution, with a fake Windows Defender antivirus theme that tricks the victim into enabling Excel macros (by clicking on "Enable Editing" or "Enable Content" buttons).

As its functionalities extended beyond being a banking trojan, it was used in ransomware operations, similar to Emotet and Trickbot, often in initial stage infections that allow attackers to carry out post-exploitation operations using frameworks such as Cobalt Strike to deliver ransomware.[125] Its operators have an active affiliate program, and are known to work with ransomware gangs including MegaCortex and ProLock. It made headlines when it was used to attack Diebold Nixdorf, a major provider of automatic teller machines (ATMs) in May 2020.[126]

5.2.2.3.3 Emotet

Emotet, also known as Geodoo or Heodo,[127] was a banking trojan that was first identified in 2014. The initial version was designed to steal banking accounts by intercepting browser traffic. Its main infection vector was email spam, typically with a malicious link in the message, or inside a PDF attachment, or an office document attachment with malicious macros. Offered as Malware-as-a-Service, it has evolved and, taking advantage of its modular/multi-component design, its functionalities were extended so it could also deliver other payloads. Its evolution included the addition of modules with functionalities to collect email addresses in Outlook, steal the contents of email messages themselves, send email spam messages independently, and spread over wireless networks. In later campaigns, stolen contents of email messages were found to be used to make email spam look legitimate to lure users. Initial targets of Emotet were German and Australian users, and later campaigns also targeted other users from different countries. Among the payloads it delivered were Qakbot, IcedId, Trickbot, and Panda. In August 2018, the first report of Ryuk ransomware infection appeared. In later infections of Ryuk, researchers have discovered that the chain of infection started with Emotet delivering Trickbot as a second payload, which eventually installed Ryuk. The combination of Emotet and Trickbot has been observed to be very effective for cybercriminals in delivering Ryuk, which targeted high profile victims.[128]

According to sources, the estimated price of the Emotet distribution service is around $2000.[129]

In January 2021, Europol announced that investigators have taken control of the Emotet infrastructure in an international coordinated action with Europol and Eurojust, together with authorities in the Netherlands, Germany, the United States, the United Kingdom, France, Lithuania, Canada and Ukraine. The Emotet operation has played a big role in the cybercrime world, as it provided its services to other cybercriminals to deliver other malware such as Trickbot, Qbot, IceID, and most dangerously Ryuk ransomware. Massive Emotet spam campaigns included a variety of different lures to trick users into opening malicious attachments or clicking on links to download malicious documents. During the years, it has used fake invoices, shipping notices, news-related and Coronavirus information as themes to present itself

[125] https://cybersecurity.att.com/blogs/labs-research/the-rise-of-qakbot
[126]https://www.bleepingcomputer.com/news/security/prolock-ransomware-teams-up-with-qakbot-trojan-for-network-access/
[127] https://malpedia.caad.fkie.fraunhofer.de/details/win.emotet
[128] https://securelist.com/the-chronicles-of-emotet/99660/
[129] https://research.checkpoint.com/2018/emotet-tricky-trojan-git-clones/

in email spam. The infrastructure used by its operation involved several hundreds of servers across the world, having different functionalities to manage infected machines, to spread new payloads, to serve other groups of criminals and to make the network resilient against takedown attempts.[130]

5.2.2.3.4 Ursnif (Gozi)

Gozi (aka Ursnif) is one of the oldest and most widely spread banking trojans in the wild since 2006. It was being offered as a Malware-as-a-Service under the name "76service".[131]

It originally started as a banking trojan that steals data from infected users, and grew into a multi-purpose platform with its modularised trojan code design. The known author, Nikita Kuzmin, was working on coding spyware and RATs and borrowed the code base from an existing trojan named Ursnif. He was also known to have access to the source code for several crimeware kits with overlapping state-of-the-art capabilities, and created a repository (together with other malware authors) under version control for a crimeware kit codebase incorporating all of these best features, which became known as Gozi. In 2010, the source code of Gozi was leaked and other threat actors have used the code to write new versions of it, which went under the names Gozi Prinimalka, Neverquest and Gozi "ISFB". A few years later, it was reported that the source code for the "ISFB" had been leaked, which gave rise to more variants under the names GozNym, Dreambot and Saigon, and subsequently to new versions that were named Goziv3 (RM3 loader), ISFB3 and Gozi2RM3(IAP 2.0). Gozi strains are known for a man-in-the-browser attack that steals the victim's credentials for a list of pre-configured websites (typically banks, and configured by actors at every campaign).[132]

Gozi variants have been reported to be distributed until today by email spam with malicious office document attachments,[133] and also by exploit kits.[134] Some known targets of its campaigns were German, English, Polish and Italian users.[135]

5.2.2.3.5 Neverquest

Neverquest, aka Vawtrak orSnifula, is one the banking trojans that emerged after the leak of the Gozi source code. According to statistics from AVG in 2015, infections by this malware were most prevalent in the Czech Republic, USA, UK and Germany. It was delivered through email spam, exploit kits or downloaded by other malware. Its capabilities include disabling antivirus products of infected machines, stealing passwords, digital certificates, browser history and cookies, logging keystrokes, taking screenshots, and communicating with remote CnC servers to send stolen data, receive updates and commands for execution. It also implemented the capability to send and receive data through encrypted favicons spread over the anonymising Tor network to hide its updates.[136]

[130] https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
[131] https://www.secureworks.com/research/gozi
[132] https://research.checkpoint.com/2020/gozi-the-malware-with-a-thousand-faces/
[133] https://www.malware-traffic-analysis.net/2021/06/18/index.html
[134] https://blog.malwaremustdie.org/2013/02/the-infection-of-styx-exploit-kit.html
[135] https://www.malware-traffic-analysis.net/2020/index.html
[136] http://securityaffairs.co/wordpress/35308/malware/vawtrak-steganography-favicon.html

In 2019, its author was arrested and was sentenced to 4 years in prison in the United States.[137]

5.2.2.3.6 Dridex

Dridex was a banking trojan that appeared in late 2014. It was derived from the Zeus trojan, and steals personal information and gains access to bank accounts.[138] It was usually distributed through email spam, with malicious office document attachments such as Word or Excel files that download its executable, and was also delivered via exploit kits.[139]

Dridex is also one of the banking trojans that evolved its functionality to provide a malware delivery service. Its infections served as an initial foothold in ransomware attacks, following the examples set by Emotet and Trickbot.

In the past, it has been known to deliver the Locky ransomware to random or any type of users via spam campaigns. It collects information about the infected system, contacts its CnC server, and is capable of downloading and executing arbitrary modules on command. In the past years, it has also been used by threat actors to deliver BitPaymer or the DoppelPaymer ransomware strains for more targeted attacks against high-value targets.[140]

5.2.2.3.7 Zbot (Zeus)

Zeus malware operates on almost all Microsoft Windows OS systems and is designed to infect the system despite the access rights of the victim. Zeus took part in botnets that were used to capture saved credentials and steal personal information from victims by intercepting and analysing the network traffic. Zeus also has keylogging capabilities, even when the victim uses a virtual keyboard, by capturing and analysing screen dumps[141]. Zeus is spread mainly through drive-by downloads and phishing schemes[142] and is also used to install additional malware on the system.[143]

Zeus source code, binary files and support services can be found for sale in underground markets at prices that can reach as much as $500 US (Goncharov, 2012).

5.2.2.3.8 Fareit

Fareit, aka Siplog or Pony, is known to steal information such as credentials and account information from FTP clients, cryptocurrency wallets and stored passwords in browsers. It has a significant history associated with malware distribution and was first detected in 2012.[144]

Versions of its source code were leaked in 2012 and 2015. Its usage and capabilities have grown and its latest versions have improved, including anti-debugging, anti-analysis, and packing. Its components have been identified and broken into three parts, namely the Pony Builder, Pony Bot, and the server-side control panel. The Pony builder is used to create the Pony Bot, or client that is downloaded by the target systems. The control panel is used by the attackers to manage the information returned by the Bot. Its common infection vectors are email spam, DNS

[137] https://securityaffairs.co/wordpress/94243/cyber-crime/neverquest-author-sentence.html
[138] https://blog.f-secure.com/a-new-variant-of-dridex/
[139] https://isc.sans.edu/forums/diary/Throwback+Friday+An+Example+of+Rig+Exploit+Kit/26990/
[140] https://www.zdnet.com/article/the-malware-that-usually-installs-ransomware-and-you-need-to-remove-right-away/
[141] https://www.enigmasoftware.com/keyloggerzeus-removal/
[142] https://usa.kaspersky.com/resource-center/threats/zeus-virus
[143] https://en.wikipedia.org/wiki/Zeus_(malware)
[144] https://www.virusbulletin.com/virusbulletin/2012/12/new-tricks-ship-zeus-packer

poisoning and exploit kits. It is commonly associated with CVE-2017-11882, which is one of the most exploited vulnerabilities from 2016-2019.[145] It has been observed to deliver Necurs,[146] Zeus and Cryptolocker.[147]

5.2.2.3.9 Dyre

Dyre, also known as Dyreza, Dyzap, and Dyranges, is a banking trojan known to steal banking and credit card information. It was first seen in mid-2014, and has been in constant development, so it has become very sophisticated and easy to use for cybercriminals to achieve financial gains. Its campaigns are well known to involve the Cutwail botnet, which distributes Dyre through email spam, with links to Dropbox and Cubby file storage services to deliver Dyre as payload. Later, threat actors shifted to use Upatre, another trojan downloader that was first documented in 2013, for the distribution of various trojans such as Dridex, Locky, GameOver, Zeus and others. Upatre-Dyre campaigns involve massive spam campaigns, typically disguised as invoice message notification with an attachment or link that will eventually download the payload. Upatre was the top malware delivered through spam in the first half of 2014, according to Trend Micro. Once Dyre is downloaded and executed, it performs man-in-the-middle attacks through browser injections, steals users' banking credentials, logs keystrokes, and has other features that allow an attacker to perform fraudulent activities.[148]

In 2014, it was used in a large-scale, credential-phishing campaign that targeted big financial groups, including Bank of America, Citigroup, Royal Bank of Scotland and JPMorgan Chase customers. This time, the attack was focused on searching for sensitive business data and accessing organisational systems.[149]

Dyre was also notable for an attack that successfully stole more than $1 million from targeted enterprise organisations in April 2015. The attack used a sophisticated social engineering technique, where the attacker displayed a message on the screen of the infected machine while the user was logging to bank websites. The message explained that the site was having issues and the victim should call a specified number to get help. This resulted in the victim calling the number and providing the organisation's bank credentials. This allowed the attacker to make the wire transfers, while launching a DDoS attack against the victim.[150]

In November 2015, Dyre operations became quiet when researchers observed that Dyre campaigns and control infrastructure had become inactive. Around the same time, Russian authorities conducted a raid on offices associated with a Moscow film company as part of cracking down on financial hacking operations. There were, however, no direct links to confirm a connection between Dyre's inactivity and the conducted raid.[151]

[145] https://www.hhs.gov/sites/default/files/pony-fareit-malware.pdf
[146] https://www.mysonicwall.com/sonicalert/searchresults.aspx?ev=article&id=670
[147] https://archive.f-secure.com/weblog/archives/00002655.html
[148] https://blog.trendmicro.com/trendlabs-security-intelligence/cutwail-spambot-leads-to-upatre-dyre-infection/
[149] https://securityintelligence.com/dyre-banking-trojan-used-in-apt-style-attacks-against-enterprises/
[150] https://securityintelligence.com/dyre-wolf/#.VR564eG0CL1
[151] https://www.bankinfosecurity.com/report-dyre-crackdown-in-moscow-a-8853

5.2.2.4 Rootkits

Rootkits traditionally referred to a maliciously modified set of administrative tools that granted "root" access to the attacker and other unprivileged programs run on the system. Modern rootkits are used to make other software payload undetectable by adding stealth capabilities and are designed to stay hidden themselves.[152] Rootkits have access to all kernel space elements, such as processes, registry entries, memory and network connections, thus granting full control over a computer to the criminal. As an example, rootkits are used to deactivate antimalware protection running on systems and to hide malicious activity, facilitating ongoing attacks and cybercrime operations.

Rootkits are quite expensive and rare in marketplaces compared to other malware. A Linux rootkit that replaces common commands can cost about $500 US and a Windows rootkit that operates at the driver level can cost up to about $300 US (Goncharov, 2012).

There are also open-source rootkits freely available on the web. With one of these, a threat actor does not even have to go to the underground market. An attacker can just use readily available code and modify it to create his own variants of rootkit.[153]

5.2.2.4.1 Sality

Sality is a polymorphic virus that infects executable files on local, shared and removal drives. It was first detected in 2003. Over the years, threat actors have modified it to add new features, such as rootkit and backdoor functionalities. It can download and run additional trojans, and steal data from the infected machine. Later variants also included the capability to communicate over a peer-to-peer (P2P) network, allowing an attacker to control machines infected with Sality using a botnet.[154]

The Sality botnet was found to be used by attackers to perform distributed attacks, such as sending spam and attacking routers. One of the notable features of Sality was having a DNS changer component that finds administration pages for routers and performs brute force password attacks in order to change the router's primary DNS server settings. Modification of the server settings will then lead the users behind the router to go to a fake Chrome installer page, which installs Sality itself, whenever "facebook" or "google" domains are resolved.[155] According to IBM, Sality was one of the 10 most common file infectors in 2011 and 2012.[156]

5.2.2.4.2 Alman

Alman, also known as Almanahe and PE_CORELINK, is a virus that infects executable files and has rootkit capabilities. It propagates over the network by accessing network shares using the Administrator account name, and brute forcing a password from a predefined list of common passwords. Its capabilities include contacting a remote server to send information about the infected machine.[157]

[152] https://en.wikipedia.org/wiki/Rootkit#Uses
[153] https://www.virusbulletin.com/virusbulletin/2005/09/trouble-rootkits/
[154] https://www.f-secure.com/v-descs/virus_w32_sality.shtml
[155] https://www.welivesecurity.com/2014/04/02/win32sality-newest-component-a-routers-primary-dns-changer-named-win32rbrute/
[156] https://www.ibm.com/services/business-continuity/cyber-attack
[157] https://www.f-secure.com/v-descs/virus_w32_alman_a.shtml

5.2.2.4.3 Necurs

Necurs is a kernel-mode driver component that was first seen in May 2011. Its earliest version came as standalone malware until 2012, when it was observed to be dropped by a trojan downloader, which was also called Necurs. It was notable for being incorporated into the Gameover Zeus botnet in late 2014, as a protective mechanism to prevent removal of malware from infected machines. The Gameover Zeus botnet was estimated to run into hundreds of thousands of infections at that time, and was mainly used for online banking theft.

The rootkit's design was interesting according to published research, as it did not require any changes by the author to be added to an existing threat such as the Gameover Zeus. Its features were essentially designed to make the driver well suited for use by other cybercriminals, which led it to be considered as "crimeware for hire", better known as "Malware-as-a-Service".[158]

5.2.2.4.4 Rustock

Rustock, also known as Mailbot, is a kernel-mode rootkit that modifies the kernel to hide its presence on the infected machine. It contains a user-mode DLL in an encrypted format as payload. Once the driver has been initialised in the infected machine, it extracts the DLL payload and executes it. The payload was identified to be a spambot with backdoor capabilities.[159]

According to Kaspersky's research the distribution of Rustock had begun in September 2007, by a group of cybercriminals, under the name IFrameBiz, whose operations and members are believed to be from Russia. The group's botnet at that time included millions of computers infected with various trojan downloaders that can instantly deliver any new payloads. The group was also known to exist since 2004.[160]

5.2.2.4.5 ZeroAccess

ZeroAccess is a kernel-mode rootkit that uses advanced techniques to hide its presence. It is capable of running in both 32- and 64-bit versions of Windows with a single installer and acts as a platform for malware delivery. It was mainly distributed by the Blackhole exploit kit, and also arrived as part of trojanised software, such as installers for a game, or programs such as cracks and keygenerators.[161]

One of its main payloads was known to be click fraud malware. The malware allows infected machines to perform HTTP requests to specific URLs, abusing the pay-per-click arrangement with a webmaster who publishes clickable ads from advertisers, who then pay every time a visitor clicks on the ad. The click fraud malware was tightly bound to ZeroAccess itself, based on its characteristics. Another payload was a spambot that downloads spam templates and targets email addresses to send spam. It is most likely that the spambot author rents a portion of the ZeroAccess botnet to deliver their own malware.[162]

5.2.2.4.6 Sinowal (the Bootkit)

[158] https://archive.f-secure.com/weblog/archives/00002717.html
[159] https://www.f-secure.com/v-descs/mailbot_az.shtml
[160] https://securelist.com/rustock-and-all-that/36217/
[161] https://nakedsecurity.sophos.com/zeroaccess2/
[162] https://nakedsecurity.sophos.com/zeroaccess4/

Sinowal, also known as Bootkit, is a rootkit that infects the Master Boot Record (MBR) and is thus able to load its driver before the operating system starts. It first appeared at the end of 2007, and was found distributed through compromised sites, porn resources and pirate software sites. When the user visits the website, a specially crafted script will start to run, which will redirect the user to a customised exploit. The customised exploit was generated through a crimeware tool Neosploit administrative panel, which provides a bundle of exploits that has been known since the middle of 2007. It was being sold on the black market for a few thousand dollars (between $1000 and $3000). Upon successful exploitation, the bootkit will be launched, which then modifies the boot sector and places the main body of the malicious program on the hard disk sectors. Once installed, the bootkit connects to a command and control server, downloads a DLL module as an encrypted packed instance, decrypts it and loads it in the memory. The DLL module is an infostealer, which is the main functionality of Sinowal. Once infected, it then tries to steal passwords from different applications, such as Total Commander, Thunderbird, FlashFXP, SecureFX, FTP clients, and many more. Most of the applications were related to web site administration, which suggests that it may be trying to gather sites it can use to host the botnet or to host exploits. It also steals bank accounts by intercepting traffic to banking websites. The module was capable of launching a man-in-the-middle attack by using the bootkit as a platform that had full access to the resources of the operating system. At the time the of incident, investigations found five main servers were used to download the exploits, with over 200,000 users from the United States visiting the servers over a period of 24 hours.[163]

5.2.2.4.7 TDSS

TDSS is a rootkit that was first detected in April 2008. It is basically a universal rootkit that can hide any malicious program and offer higher privileges on the victim's machine. Rootkit features include registry and file hiding, code injections, TCP network port hiding, and function executions that can terminate processes, and hide injected DLLs. Its framework was updated, and later versions included infecting selected system driver files, particularly the MiniPort/Port Driver. This enabled the rootkit to load as soon as the operating system started.

TDSS was distributed through affiliate programs to deliver rogue antivirus software at that time. It implements a Trojan clicker and imitates a user in going to websites by creating a browser window. It then creates popup windows for rogue antivirus programs or any site the botnet owner defines.[164]

5.2.2.5 Keyloggers

A keylogger is software that captures keystrokes entered on a computer. Keyloggers are used to capture credentials, communications, and any other information for purposes that may include fraud or espionage. Keyloggers are often commercially available in the underground market, allowing an actor with no technical knowledge to record and steal information from a victim's machine.

5.2.2.5.1 Phoenix keylogger

The Phoenix keylogger emerged at the end of July 2019. The keylogger is offered as Malware-as-a-Service, sold for $14.99-25.00 per month in the underground market. Its features include

[163] https://securelist.com/bootkit-the-challenge-of-2008/36235/
[164] https://securelist.com/tdss/36314/

defensive and evasive mechanisms to avoid analysis and detection by security products. Aside from the keylogging module, it steals credentials from browsers, mail clients, FTP clients and chat clients. It sends stolen data via SMTP and FTP exfiltration protocols, and in some cases, through Telegram, a popular chat application that is also used by cybercriminals for its legitimacy and end-to-end encryption. Campaigns delivering the Phoenix keylogger are usually email spam with malicious RTF or Microsoft office documents abusing the known Equation Editor vulnerability (CVE-2017-11882).[165]

5.2.2.5.2 Ardamax

Ardamax keylogger is a commercially available surveillance package. It was notable for being used by threat actors dubbed as "TeamSpy crew" who targeted government organisations throughout the Commonwealth of Independent States (CIS) and Eastern European nations in 2010. The operation involved using a legal software TeamViewer as main toolset to infiltrate and steal data from targets, and deployed several tools such as commercial keyloggers like Ardamax.[166]

5.2.2.5.3 HawkEye

HawkEye, also known as HawkEye Reborn, is a keylogger that was first discovered in 2013. It was believed to be a derived from Predator Pain keylogger which was first advertised for 35$ on the underground market.[167]

It was delivered mostly via email spam campaigns, having themes such as notification, shipping, purchases, invoice and many others to lure users. Targeted countries were the United States, Australia, Canada, Thailand, Taiwan ROC, Kuwait, Japan, Spain, Italy and Sweden. The top targeted areas were technology, education, manufacturing, professional and legal services, transportation and logistics, wholesale and retail, construction, media and entertainment, telecommunications and government.[168]

5.2.2.5.4 iSpy

iSpy is a keylogger written in .Net 2.0 that was discovered in 2016. It was sold in the underground market in different packages, with prices ranging from $25, $35 and $45 for monthly, bi-yearly and yearly subscriptions. On top of its keylogging capabilities, its features include stealing passwords, screenshots, and monitoring webcams and clipboards. It also has the capability to terminate security products to avoid being detected and blocked. It was delivered via email spam campaigns with malicious JavaScripts or documents as attachments.[169]

5.2.2.6 Ransomware

Ransomware is a special type of malware that targets the victim's data by blocking access to it and/or threatening to make it publicly available. After an asset or a computer is compromised, the criminal demands a ransom from the owner. Typically, the ransomware encrypts the hard

[165] https://www.cybereason.com/blog/phoenix-the-tale-of-the-resurrected-alpha-keylogger
[166] https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/20134928/theteamspystory_final_t2.pdf
[167] https://stopmalvertising.com/malware-reports/analysis-of-the-predator-pain-keylogger.html
[168] https://unit42.paloaltonetworks.com/surveillance-malware-trends-tracking-predator-pain-and-hawkeye/
[169] https://www.zscaler.com/blogs/security-research/ispy-keylogger

drive of a computer and requires a ransom to provide the key for the decryption. In such cases, namely in cryptoviral extortion attacks, recovering the files without the decryption key is an intractable problem. Ransoms are paid via digital currencies and cryptocurrencies, thus making tracing extremely difficult for authorities.

New ways of pressuring victims to pay the ransom have been introduced. Primitive versions of ransomware had only destructive behaviour and tended to leave the data in an irreversibly corrupted form, or erased them from storage drives. Now, once criminals gain access to the system, they exfiltrate the data before delivering the ransomware. Criminals then threaten to publish sensitive data online or sell it to the highest bidder through auctions. Breach of data or disclosure of personal information can lead to GDPR data compliance issues and therefore GDPR fines, but also result in the victimisation of individuals.

As of today, ransomware remains one of the most dominant threats, especially for public and private organisations within as well as outside Europe (Europol, 2020). It has a major impact, both on its primary targets and on those whose data is compromised, even if they are not both attacked directly. Consequently, as an indirect threat, ransomware attacks may be directed against third-party providers that play a key role in the supply chains of other major organisations. These attacks have an impact across the whole chain of suppliers and clients, damaging all these organisations.

Ransomware attacks are also becoming more sophisticated and targeted. The level of sophistication varies across threat actors. On the one hand, reports mention cases of lone actors, sometimes without expertise, that make use of CaaS products to conduct their attacks and demand ransoms up to a few thousand euros. On the other hand, there are organised crime groups with advanced technical expertise, focusing on high value targets and demanding ransoms up to millions of euros.

Sophisticated and highly targeted attacks start with a preparation stage where the victim is observed and information is gathered. After carrying out adequate reconnaissance on the victim's system, criminals exploit the system and stay idle until the ideal time comes to enable the ransomware. Internal communications are continuously monitored to identify key moments in the organisation when the attack will cause the biggest impact. This strategy maximises the impact on victims, thus increasing the ransom amount requested and the possibility of getting the ransom paid.

Ransomware spreads in similar ways to other types of malware. These ways include visiting malicious websites, downloading and running malicious attachments, installing fake updates or malicious software and connecting infected external devices to your computer system.

Ransomware operations are often seen as a service in the Dark Web. The creators of the malware, distribute the software for free to other people in the cybercrime chain (affiliation program). The affiliates spread and install the malware and receive a portion of the ransom.

Since the first known ransomware attack occurred in 1989 (AIDS trojan) and targeted the healthcare industry, the world has experienced many attacks over the last years:

5.2.2.6.1 WannaCry

In May 2017, WannaCry spread through the internet and across 150 countries using the DoublePulsar backdoor along with the EternalBlue Windows vulnerability, which was

allegedly created by the U.S National Security Agency and leaked by the Shadow Brokers group. Reportedly, more than 200,000 computers were infected, and a ransom was demanded by their users in the form of the Bitcoin cryptocurrency.

WannaCry encrypted valuable files, making them unavailable to their users. The attackers initially demanded a ransom of $300 US but later doubled the ransom to $600 US. The malware advertised that encrypted files would be permanently deleted unless victims paid the ransom within a few days. The fact is that most of those who paid the ransom were unable to recover their data, because of a fault in the code that was used to associate the payment with a specific victim's computer.

WannaCry affected Telefónica and several other large companies in Spain, as well as a third of hospital trusts in the UK, costing the NHS an estimated almost £100m.[170] Other popular victims were FedEx, Deutsche Bahn, Hitachi, Honda, Renault, as well as the Russian Interior Ministry and Russian telecom operator MegaFon.

The discovery of a kill switch domain name[171] and the fact that Microsoft rapidly released emergency security patches for Windows, even for older unsupported versions,[172] prevented infected computers from spreading WannaCry further and managed to halt the attack within a few days of its discovery.

5.2.2.6.2 Petya/NotPetya

Petya was first discovered in March 2016 and targeted Windows systems. Initial versions installed a custom boot loader that overwrote the existing MBR and then encrypted the master file table, which is used as a roadmap for the hard drive. Consequently, the user's files remained intact but the part of the system that contained the location of the files in the drive was affected. At this point, the system was prevented from booting and the ransomware demanded a ransom though a Bitcoin payment in order to decrypt the hard drive.

Petya spread through human resources departments via a fake job application email with an infected package. This package contained a stock image of a young man and an executable file which was the actual malware. The Petya ransomware infected millions of people during its first year of its release.

In June 2017, a new variation of the malware emerged and began to spread rapidly, initially in Ukraine but soon across Europe and beyond. Kaspersky Lab reported that the majority of infections targeted Russia and Ukraine, where more than 80 companies were initially attacked, including the National Bank of Ukraine. This variation was named NotPetya (aka ExPetr) by Kaspersky, as it had major differences in comparison to its predecessors, such as its capability to spread very quickly using the same EternalBlue exploit that was used by WannaCry.

NotPetya had a destructive motive, rather than a financial one, as it was designed more as a wiper and not as traditional ransomware, where there is a way to generate a usable key to decrypt data.[173] In addition, the screen of NotPetya displayed a randomly generated identifying

[170] https://www.zdnet.com/article/this-is-how-much-the-wannacry-ransomware-attack-cost-the-nhs/
[171]https://www.theguardian.com/technology/2017/may/15/accidental-hero-who-halted-cyber-attack-is-22-year-old-english-blogger
[172]https://www.zdnet.com/article/wannacrypt-ransomware-microsoft-issues-patch-for-windows-xp-and-other-old-systems/
[173] https://www.bbc.com/news/technology-40442578

number to the victims. This identifying number (installation ID) is used by criminals to identify which victim has paid the ransom in order to send the key for the decryption. Experts believed that NotPetya attacks were politically-motivated against Ukraine, since they occurred on the eve of the Ukrainian holiday Constitution Day.[174]

5.2.2.6.3 Ryuk/Conti

Ryuk was a piece of ransomware that was used in high-profile targeted attacks globally, where the threat actors took time to carry out reconnaissance inside an infected network, identified and targeted critical network systems to maximise the impact of the attack, and demanded large amounts of ransom. It was one of the leading ransomware families and was reported to generate roughly $61m between February 2018 and October 2019.[175] It was first discovered in the wild in August 2018, and was attributed to a cybercriminal group named CryptoTech, which was observed selling Hermes 2.1 in an underground forum in August 2017.[176]

According to industry reports, in early 2019 Ryuk infections were commonly seen to be linked with Emotet arriving through email spam, which distributed Trickbot as part of the infection chain. Trickbot subsequently deploys post-exploitation tools, such as Mimikatz and PowerShell Empire modules, to facilitate harvesting credentials, remotely monitor the victim's workstation and perform lateral movement to other machines within the network. These initial stages of infection enable the attacker to assess whether the victim presents a ransomware opportunity before deploying Ryuk. Ryuk also has the ability to enumerate network drives and resources and delete shadow copies, which makes recovery difficult.[177] In 2020, another loader named BazarLoader was also observed delivering Ryuk.[178]

In July 2020, researchers noticed that Ryuk was no longer being used, but new ransomware named Conti was observed to be deployed by the same ransomware operators in multiple incident response cases. It is believed that Conti is Ryuk's successor, as there were also similarities with the code, ransomware note, and the Trickbot distribution method as an attack vector.[179] Conti ransomware operators also steal sensitive documents before encrypting them and threaten their victims with leaking them if they do not pay the demanded ransom. It released its own data leak site in August 2020 and threat actors called victims on the phone to put pressure on them to pay the ransom.[180]

Ryuk and Conti targeted large organisations, including hospitals, newspapers, oil and gas companies, large engineering and construction services firms, city and county government offices, financial software providers, and food and drink manufacturers.[181]

[174] https://www.nytimes.com/2017/06/27/technology/ransomware-hackers.html
[175] https://www.zdnet.com/article/fbi-ransomware-victims-have-paid-out-140-million-one-version-has-cost-them-the-most/
[176] https://www.virusbulletin.com/virusbulletin/2019/10/vb2019-paper-shinigamis-revenge-long-tail-ryuk-malware/
[177] https://www.ncsc.gov.uk/news/ryuk-advisory
[178] https://blog.malwarebytes.com/videobytes/2020/12/videobytes-ryuk-ransomware-targeting-us-hospitals/
[179] https://www.bleepingcomputer.com/news/security/conti-ransomware-shows-signs-of-being-ryuks-successor/
[180] https://www.zdnet.com/article/ransomware-gangs-are-now-cold-calling-victims-if-they-restore-from-backups-without-paying/
[181] https://securityintelligence.com/articles/ryuk-ransomware-operators-shift-tactics/

5.2.2.6.4 CryptoLocker/CryptoWall/TorrentLocker

CryptoLocker was one of the most profitable ransomware strains of its time, and was active from 5 September 2013 to late May 2014.[182] The attack utilised a trojan that targeted Windows systems and propagated via infected email attachments and via the Gameover ZeuS botnet.[183]

CryptoLocker encrypted specific types of files stored on local and network drives on the compromised systems and then displayed a message that data would be decrypted if the ransom was paid by a specific date.[184] If this deadline was not met, the malware demanded a higher amount from the victims for getting their files decrypted.

CryptoLocker infected more than 250,000 systems[185] and earned more than $3 million US[186] before the Gameover ZeuS botnet was taken offline, by an international operation called Operation Tovar, in June 2014. During the operation, the database of private keys used by CryptoLocker was made public and many victims managed to recover their files.

CryptoWall and TorrentLocker, which were initially observed in September 2014, are popular clones of the original CryptoLocker payload and operate in a similar manner. CryptoWall and its variants have caused over $325 million US in damages[187] by asking the victims to pay about $1000 US worth of Bitcoin once the encryption is complete.[188] Similarly, TorrentLocker demands from the victim an amount that usually starts at around $420 US (in today's currency) within 3 days.[189]

5.2.2.6.5 Dharma/CrySIS

Dharma, aka CrySIS, is a piece of ransomware that was first seen in 2016. It was delivered through several infection vectors, such as email spam, fake installation files disguised as legitimate software, and most commonly, manually delivered through unsecured RDP (Remote Desktop Protocol) ports. After a successful RDP-based attack, Crysis was observed to uninstall security software on the system. It also deletes all the shadow copies before encrypting files, which makes recovery difficult after infection.[190]

It is known for targeting small businesses, but also infected several larger organisations, such as Texas Hospitals in 2018.[191]

[182] https://en.wikipedia.org/wiki/CryptoLocker
[183] https://www.f-secure.com/v-descs/trojan_w32_cryptolocker.shtml
[184]https://www.computerworld.com/article/2485214/cryptolocker-how-to-avoid-getting-infected-and-what-to-do-if-you-are.html
[185] https://www.bbc.com/news/technology-25506020
[186] https://www.bbc.com/news/technology-28661463
[187] https://www.cyberthreatalliance.org/wp-content/uploads/2018/02/cryptowall-report.pdf
[188] https://www.varonis.com/blog/cryptowall/
[189]https://www.welivesecurity.com/2014/12/16/torrentlocker-racketeering-ransomware-disassembled-by-eset-experts/
[190]https://blog.malwarebytes.com/threat-analysis/2019/05/threat-spotlight-crysis-aka-dharma-ransomware-causing-a-crisis-for-businesses/
[191] https://www.zdnet.com/article/texas-hospital-becomes-victim-of-ransomware-patient-data-potentially-leaked/

5.2.2.6.6 DoppelPaymer/BitPaymer/Grief

DoppelPaymer is a version of ransomware that first appeared in 2019 and was used in targeted attacks. It is believed to be derived from BitPaymer ransomware, having similarities with the code, ransom note and TOR-based payment portals, while having differences in its file encryption methods. DoppelPaymer was known to use ProcessHacker modules (an open-source admin utility) to terminate processes that might hinder file encryption, including software security processes. DoppelPaymer was found linked with Dridex malware as its infection vector.[192]

Threat actors behind DoppelPaymer also steal sensitive documents before encryption, and threaten victims with leaking them if they don't pay the ransom demand. It is one of those ransomware gangs that maintain a leak site for their victims. In addition, the threat actors have followed ransomware infections with intimidating calls to the victims to extort payments, or threaten to release exfiltrated data, which was observed as of February 2020.[193]

Since May 2021, its activity seemed to significantly drop and no new victims have been posted on their leak site. In the same month, though, new ransomware with the name Grief (aka Pay) appeared, with a ransom note pointing to the DoppelPaymer ransom portal. It is believed that this is a new version of DoppelPaymer, and threat actors might be rebranding the name of the ransomware as a diversion.[194]

DoppelPaymer targeted critical industries worldwide, including healthcare, emergency services and education, interrupting citizens' access to services. Its threat actors demand ransom ranging from six to seven figures in Bitcoin (BTC).[195]

5.2.2.6.7 Maze/Egregor/Sekhmet

Maze ransomware was discovered in May 2019.[196] The threat actors behind Maze introduced an additional way of extorting ransomware victims, by stealing documents before encrypting them and threatening to publish them if their victims refused to pay the ransom. In addition, it also called victims over the phone to add more pressure to pay the ransom. It was believed to be a variant of the ChaCha ransomware and it uses ChaCha20 and RSA encryption algorithms to encrypt files. It was mainly distributed through email spam, with malicious Word and Excel document file attachments, and manually by RDP brute force attacks. It was also initially delivered via the Fallout and Spelevo Exploit kits, and was seen to use exploits against Pulse VPN and the Windows VBScript Engine Remote Code Execution Vulnerability to get into a network.[197]

It also adopted the use of a virtual machine, similar to RagnarLocker ransomware, to evade detection by endpoint protection. The attack involved deploying a VirtualBox and a weaponised virtual machine with the actual Maze payload, attempting to launch the attack from within the

[192] https://www.crowdstrike.com/blog/doppelpaymer-ransomware-and-dridex-2/
[193] https://www.zdnet.com/article/fbi-says-doppelpaymer-ransomware-gang-is-harassing-victims-who-refuse-to-pay/
[194] https://www.zscaler.com/blogs/security-research/doppelpaymer-continues-cause-grief-through-rebranding
[195] https://www.ic3.gov/Media/News/2020/201215-1.pdf
[196]https://www.bleepingcomputer.com/news/security/maze-ransomware-says-computer-type-determines-ransom-amount/
[197] https://blog.malwarebytes.com/threat-spotlight/2020/05/maze-the-ransomware-that-introduced-an-extra-twist/

VM.[198] Maze ransomware attacks affected and threatened businesses and large organisations, including high profile victims such as Cognizant (one of the biggest providers of IT services in the world), Canon, Xerox and the City of Pensacola.[199]

On November 1, 2020, the threat actors behind Maze announced retirement on their leak website, and had cleaned up its data leak site before the announcement. In mid September of the same year, a new ransomware named Egregor began operating, just as Maze started to shut down operations. Egregor is believed to be the same underlying software as Maze and Sekhmet ransomware, as they share similar ransom notes, payment site naming and code. This was also confirmed by a threat actor, according to one report.[200]

5.2.2.6.8 REvil/Sodinokibi/GandCrab

GandCrab ransomware was discovered in early 2018. It is one of the most popular and prevalent kinds of ransomware that came as part of the Ransomware-as-a-Service (RaaS) business model used by ransomware developers in 2018 and 2019. Its operators offered a revenue-sharing model that helped them improve the platform over the years. It was delivered through massive email spam campaigns, malvertising and exploit kits. It was also found to target managed service providers (MSPs) in order to mass-infect all of their clients in a single attack.[201]

It demanded payment in the DASH cryptocurrency and does not encrypt files if it identifies the keyboard layout of the machine to be Russian. It continued to evolve and had developed releases with improvements for each version throughout the first part of 2019. In May 2019, the operators announced that they were shutting down operations, claiming that their affiliates made $2 billion USD over the previous year and they themselves made $150 million USD.[202]

In April 2019, a new variety of ransomware appeared under the name Sodinokibi, which shared similarities with GandCrab. Compared to GandCrab's delivery vectors, Sodinoki was delivered by exploiting a vulnerability in the Oracle WebLogic Server (CVE-2019-2725), and also by RDP-brute force attacks. However, its technical similarities suggested that it was a rebrand of the GandCrab ransomware, and the difference in the distribution method suggested that targeted victims had changed, from ordinary users who might click malicious links from spam email, to companies/organisations with essential files critical to business.[203] In July 2019, "REvil" became the new name of this ransomware. Its platform offered attackers the features of malware generation, random demand and payment service, victim communication and cryptocurrency laundering. The affiliates receive an estimate of 60% to 70% of the payouts from using the platform.[204] In 2020, it started to steal files before encrypting them, to further blackmail victims by threatening to leak them if they refused to pay the ransom.

Sodinokibi/REvil has become one of the most active types of ransomware that targeted high-profile organisations and industries, including financial firms, healthcare providers, the court

[198] https://news.sophos.com/en-us/2020/09/17/maze-attackers-adopt-ragnar-locker-virtual-machine-technique/
[199] https://www.kaspersky.com/resource-center/definitions/what-is-maze-ransomware
[200] https://www.bleepingcomputer.com/news/security/maze-ransomware-is-shutting-down-its-cybercrime-operation/
[201] https://www.bleepingcomputer.com/news/security/ransomware-attacks-target-msps-to-mass-infect-customers/
[202] https://www.crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/
[203] https://blog.talosintelligence.com/2019/04/sodinokibi-ransomware-exploits-weblogic.html
[204] https://www.domaintools.com/content/It%E2%80%99s-Not-Finished-The-Evolving-Maturity-In-Ransomware-Operations.pdf

system, nuclear weapon contractors, food production plants, MSP providers, media and communication.

In July 2021, it launched one of the biggest supply chain attacks by targeting Kaseya VSA (a cloud-based MSP platform that allows providers to perform patch management and client monitoring for their customers). The attackers deployed REvil ransomware via a malicious update of "Kaseya VSA Agent Hot-fix." This affected multiple managed service providers, 60 direct customers and around 1500 downstream customers of those MSPs. The ransomware gang demanded $70 million for a universal decryptor key that would remediate all impacted victims; this was negotiated down to $50m according to reports.[205]

5.2.2.6.9 RagnarLocker

The RagnarLocker ransomware was observed in 2019 and was used in highly targeted attacks, as each sample observed was tailored for the organisation being attacked. It is commonly delivered through RDP-based attacks. In May 2020, it introduced a new attack method by deploying a virtual machine on a targeted device to hide the ransomware from endpoint security products. The attack included a package with an installer of Oracle VirtualBox hypervisor, and a Windows XP virtual disk image file. The ransomware was executed inside a virtual machine, accessing the host's local disks, mapped network and removal drives in order to encrypt them. The same method was later adopted by the Maze ransomware.[206]

RagnarLocker uses a custom stream cipher based on the Salsa20 cipher and demands ransom in Bitcoin cryptocurrency. It's operators were known to own ".onion" domains available on Tor and one Surface Web domain registered.[207] In July 2020, it started to steal files before encrypting them to further extort their victims, threatening to publish stolen data in their so-called Wall of Shame section if they refused to pay ransom. Some of the high-profile targets were Energias de Portugal (energy company) where it demanded 1580 Bitcoin (approximately $11 million US), Campari (an Italian liquor), and Capcom (Japanese gaming firm),[208] while other main targets were reported to be from the US, including IT, construction, legal, auto, energy, and media industries.

5.2.2.6.10 Darkside

Darkside ransomware was first seen in August 2020 and operates as Ransomware-as-a-Service, where profit is shared between its developers, and partners or affiliates who deploy the ransomware. As with other ransomware families, its operators also maintain its own website accessible via Tor, which they use to publish their victims and further threaten them with leaking stolen data if they do not pay the ransom demanded. Based on incident response cases, researchers have observed groups of threat actors deploying this ransomware using different infection vectors. In multiple cases, it was observed that infection started with suspicious authentication attempts against corporate VPN infrastructure, either through brute force

[205]https://www.bleepingcomputer.com/news/security/revil-ransomware-hits-1-000-plus-companies-in-msp-supply-chain-attack/
[206]https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/
[207] https://securelist.com/targeted-ransomware-encrypting-data/99255/

[208] https://www.bankinfosecurity.com/fbi-warns-uptick-in-ragnar-locker-ransomware-activity-a-15454

password attack, or by using legitimate credentials. In some incidents, it was seen to exploit a vulnerability in the SonicWall SMA100 SSL VPN product (CVE-2021-20016), and leveraged TeamViewer to obtain persistence within the victim's environment. In other cases, the ransomware was deployed through phishing emails and legitimate services to deliver a Smokedham backdoor that supports keylogging, taking screenshots and executing .NET commands. The attacks have used several tools for internal reconnaissance, lateral movement and actual deployment of ransomware within victim environments after gaining initial access, such Mimikatz, Cobalt Strike beacon payloads, PsExec, Advanced IP Scanner, BloodHound, and RDP. It was used to target organisations in more than 15 countries across different sectors, including financial services, legal, manufacturing, professional services, retail and technology.[209]

One notable victim of Darkside ransomware was the Colonial Pipeline, the biggest U.S. gasoline pipeline, in May 2021. The attack caused the declaration of a state of emergency in 18 states because of fuel outages.[210] The threat actors claimed to have stolen 100 GB of corporate data from Colonial Pipeline. They also claim to have three more victims: a construction company based in Scotland, a renewable energy product reseller in Brazil, and a technology services reseller in the US, from which they have stolen 1.9 GB of data that include sensitive information about clients, finance and employee data.

In addition to encrypting files and threatening victims of leaking stolen data if the ransomware is not paid, the threat actors also threatened victims with carrying out DDoS attacks, a new way of extortion used by threat actors using Avaddon ransomware. In addition, they also threaten to directly email the victim's customers or to have contracted call centres contact customers.[211]

5.2.2.6.11 Lockbit

Lockbit, formerly known as "ABCD" ransomware, is another piece of ransomware offered as a service that was used in high-profile attacks. According to the underground market, its development started in 2019.[212]

One of its significant capabilities is to propagate by itself within the network of a targeted organisation. Once an attacker has infected a single host, it can find other accessible hosts and connect to them and infect more hosts, using tools such PowerShell scripts and Server Message Block (SMB). It was used to target organisations in Europe, the United States, China, India, Indonesia and Ukraine.[213]

Its business model offers an affiliate program that gives up to 70-80% of the ransom payout as commission. According to reports, affiliates purchase access to networks from third-party

[209]https://www.fireeye.com/blog/threat-research/2021/05/shining-a-light-on-darkside-ransomware-operations.html
[210] https://www.fmcsa.dot.gov/emergency/esc-ssc-wsc-regional-emergency-declaration-2021-002-05-09-2021
[211]https://www.trendmicro.com/en_fi/research/21/e/what-we-know-about-darkside-ransomware-and-the-us-pipeline-attac.html
[212]https://news.sophos.com/en-us/2020/04/24/lockbit-ransomware-borrows-tricks-to-keep-up-with-revil-and-maze/
[213] https://www.kaspersky.com/resource-center/threats/lockbit-ransomware

pentesters in many cases, instead of breaching the companies by themselves. Now, its operators are trying to recruit "insiders" who can provide access to a corporate networks.[214]

One of its recent high-profile victims was Accenture, an Irish-based multinational company that provides consulting and professional services to a wide range of industries. The attackers claimed to have obtained access to the corporate's network via an "insider". Accenture stated that affected systems were restored by their backups and there was no impact on Accenture's operations.[215] However, the threat actors claimed to have stolen 6 terabytes of data and to have published 2400 files appearing on the Dark Web.[216]

5.2.2.6.12 SunCrypt

SunCrypt ransomware was first seen in the wild in October 2019. As with other ransomware offered as a service, its operators were looking for affiliates. In addition to the double extortion technique of stealing and encrypting files, it provides a DDoS that may be used as part of the extortion process to persuade victims to pay ransoms. It also maintains a data leak site where they expose their victims. SunCrypt was mostly delivered through PowerShell loaders. Similarly to other ransomware, it also deletes Shadow Volumes to make recovery difficult for the victim. Its ransom note is written in multiple languages: Spanish (Latin American Spanish), German, French and English.[217]

One of the notable victims of SunCrypt was the University Hospital of New Jersey in 2020. The attackers leaked 1.7 GB of archive which contained over 48,000 documents. The documents leaked included patients' information, and personally identifiable information such as drivers' licences, Social Security numbers, dates of birth and records relating to the Board of Directors.[218]

5.2.2.6.13 Avaddon

Avaddon ransomware started its operations in June 2020 through email spam campaigns. Its business model pays 65% of ransom payout to affiliates. According to Coveware, Avaddon's average ransom demand was around $600k. It was actively used by threat actors against a wide range of sections in the US and worldwide. Aside from the normal extortion procedure of asking for ransom to decrypt files, and leaking stolen files, it was also known for threatening victims with DDoS attack to pressure them into paying ransoms. In May 2021, the Federal Bureau of Investigation (FBI) and the Australian Cyber Security Centre (ACSC) warned organisations of campaigns involving Avaddon ransomware. The alert included more than 20 countries, and more than 16 sectors being targeted at that time. A month after the alert, Avaddon's Tor sites became inaccessible, indicating that the operation had shut down. It also released the decryption keys for its victims to BleepingComputer, a website publishing technology and cyber security

[214]https://www.bleepingcomputer.com/news/security/lockbit-ransomware-recruiting-insiders-to-breach-corporate-networks/
[215]https://www.bleepingcomputer.com/news/security/accenture-confirms-hack-after-lockbit-ransomware-data-leak-threats/
[216] https://twitter.com/EamonJavers/status/1425536526415548420
[217]https://sapphirex00.medium.com/diving-into-the-sun-suncrypt-a-new-neighbour-in-the-ransomware-mafia-d89010c9df83
[218]https://www.bleepingcomputer.com/news/security/university-hospital-new-jersey-hit-by-suncrypt-ransomware-data-leaked/

news. There was no clear reason for the shutdown, but it was speculated that it might be because of law enforcements closely monitoring its operations.[219]

5.2.2.7 Exploit kits

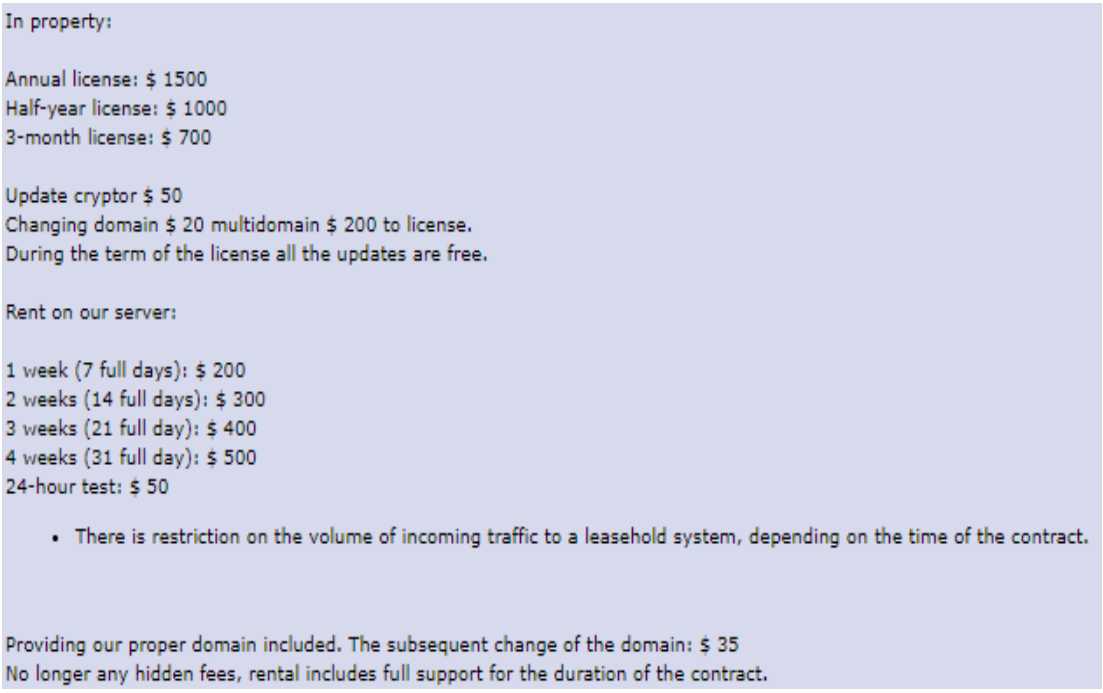
Exploit kits, or packs, are a form of crimeware that specialises in attacking software vulnerabilities. Most commonly, exploit kits are used by cybercriminals to launch drive-by-download attacks, a type of attack that allows the unintentional download of malware without the user's knowledge. Software used to browse the Internet, such as Adobe Flash, Java, Internet Explorer and Microsoft Silverlight are the most common targets of exploit kits. They are often planted by attackers on a webpage, either deliberately created by an attacker, or most commonly, on compromised web pages. In many cases, users are also redirected to exploit kit pages through massive malvertising campaigns (an attack that involves injecting malicious code into ads on websites). When the user visits the page, the exploit kit silently checks on the user's system, such as the browser version, and other plugins installed, and tries to exploit a vulnerability if one is found. Upon successful exploitation, it will proceed to deliver and execute the payload without the user being aware of it.[220]

Exploit kits have played a big role in malware distribution, including ransomware. They were most active in the years 2013 to 2015. In 2016, browser vendors such as Google Chrome, Microsoft Edge and Apple Safari started to take action to block Flash, which was the most common software targeted by exploit kits. Law enforcement agencies also tracked down threat actors behind popular exploit kits and, eventually, their level of activity dropped. They are not as prominent as they used to be, but there are still some active ones today that are used by cyber-criminals.

5.2.2.7.1 Blackhole Exploit kit

The Blackhole exploit kit was one of the most popular kits and was released on the underground market in 2010. Its business model included rental options, where cyber-criminals can pay for a hosted service, on top of other licensing options. The pricing model was documented to be as follows in 2010:[221]

[219] https://www.bleepingcomputer.com/news/security/avaddon-ransomware-shuts-down-and-releases-decryption-keys/
[220] https://www.f-secure.com/v-descs/exploit_kit.shtml
[221] http://www.malwaredomainlist.com/forums/index.php?topic=4329.0


In property:

Annual license: $ 1500
Half-year license: $ 1000
3-month license: $ 700

Update cryptor $ 50
Changing domain $ 20 multidomain $ 200 to license.
During the term of the license all the updates are free.

Rent on our server:

1 week (7 full days): $ 200
2 weeks (14 full days): $ 300
3 weeks (21 full day): $ 400
4 weeks (31 full day): $ 500
24-hour test: $ 50

- There is restriction on the volume of incoming traffic to a leasehold system, depending on the time of the contract.

Providing our proper domain included. The subsequent change of the domain: $ 35
No longer any hidden fees, rental includes full support for the duration of the contract.

Figure 7: Blackhole exploit kit advertising pricing for access and rent to exploit kit.[222]

Its campaigns involve attackers infecting websites by injecting malicious iframes or heavily obfuscated JavaScript to redirect users to a remote server. This remote server acts as a traffic manager, often referred to as a Traffic Directing Server (TDS), from where the request is bounced to the Blackhole exploit site.

Attackers also use email spam to lead users to Blackhole exploit sites. Email spam campaigns involved tricking users to click on URL links within the email message, or with an HTML attachment. The HTML attachment has obfuscated JavaScript similar to the injected JavaScript code in compromised websites that are used as redirectors.[223] The Blackhole Exploit kit was seen to be quick to include support for fresh exploits,[224] and was seen to be the most prevalent until 2013, when the author, known as "Paunch", was arrested.[225]

It has been reported that Paunch was earning $50,000 per month and had more than 1000 customers with his illegal business. He worked with other cyber-criminals to purchase new exploits that could be included in the Blackhole Exploit kit and also supported a more exclusive exploit kit called "Cool", which F-Secure researchers have found to be very similar to Blackhole.[226]

Summary of vulnerabilities exploited by the Blackhole exploit kit[227]:

[222] http://www.malwaredomainlist.com/forums/index.php?topic=4329.0
[223] https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-5/
[224] https://archive.f-secure.com/weblog/archives/00002414.html
[225] https://archive.f-secure.com/weblog/archives/00002522.html
[226] https://krebsonsecurity.com/2013/12/meet-paunch-the-accused-author-of-the-blackhole-exploit-kit/
[227] https://nakedsecurity.sophos.com/exploring-the-blackhole-exploit-kit-4/
https://securelist.com/filling-a-blackhole/57916/

Java	CVE-2012-5076
Java	CVE-2012-4681
Java	CVE-2012-0507
Java	CVE-2013-0422
Java	CVE-2009-1671
Java	CVE-2010-0840
Java	CVE-2010-0842
Java	CVE-2010-0886
Java	CVE-2010-1423
Java	CVE-2010-3552
Java	CVE-2010-3544
TrueType Font	CVE-2011-3402
Windows Help and Support Centre	CVE-2010-1885
Adobe Reader	CVE-2008-2992
Adobe Reader	CVE-2010-0188
Adobe Reader	CVE-2007-5659
Adobe Reader	CVE-2009-0927
Adobe Reader	CVE-2009-4324
Adobe Reader	CVE-2011-0559
Adobe Reader	CVE-2011-2110
Adobe Reader	CVE-2011-0611
Internet Explorer	CVE-2006-0003

Observed payloads delivered through the Blackhole exploit kit:

https://archive.f-secure.com/weblog/archives/00002414.html

Scareware: Fake AV
Banking Trojan: Zeus, Cridex (Oliver, 2012)
Rootkit: TDSS, ZeroAccess

5.2.2.7.2 Angler Exploit Kit

The Angler exploit kit first appeared in late 2013. As with most exploit kits, its operation involves compromising websites by injecting malicious html iframes or JavaScript codes to redirect user web traffic to Angler exploit sites. It was also one of the most prevalent exploit kits that has been linked to high profile malvertising and ransomware campaigns. One of the notable malvertising campaigns was attacking Yahoo's own ad network in July 2015.[228] It has been reported that the full scope of its operations could yield more than $60m annually, by delivering ransomware payload.[229]

Angler was known to use domains generated by domain generation algorithms (DGAs), as with other exploit kits. It's landing pages were highly obfuscated to evade antivirus detections. One of the main features of the Angler exploit kit is its anti-sandbox checks by using XMLDOM functionality in IE. It checks for the presence of security tools for analysis, virtual machines and sandboxes. It was known to use domain shadowing—a technique used by attackers that abuses stolen DNS records—and updates it by adding multiple subdomains that direct to the malicious exploit kit pages. Through the years it was active, it evolved by adding support for fresh exploits, including exploits for the "Hacking Team" zero-day Adobe Flash Player vulnerabilities (CVE-2015-5119, CVE-2015-5122). Its URL structure has also been changed a couple of times, evolving to make URLs look legitimate and common traffic to avoid detection by security products. Since the alleged arrest of the operators of the Blackhole exploit kit, many other exploit kits have sprung up in the underground market, and Angler was most prevalent in the years 2014 and 2015.[230]

In June 2016, Angler became inactive.[231] Researchers have speculated that the inactivity could be related to the arrests tied to a Russian hacker gang over a $25m theft.[232] The connections were not confirmed, but since then no more infections by the Angler exploit kit have been observed.[233]

Summary of vulnerabilities exploited by the Angler exploit kit:

Windows OLE	CVE-2014-6332
Jscript in IE	CVE-2015-2419
Silverlight	CVE-2015-1671

[228] https://blog.malwarebytes.com/threat-analysis/2015/08/large-malvertising-campaign-takes-on-yahoo/
[229] https://talosintelligence.com/angler-exposed
[230] https://news.sophos.com/en-us/2015/07/21/a-closer-look-at-the-angler-exploit-kit/
[231] https://blog.malwarebytes.com/threats/angler/
[232] https://www.bbc.com/news/technology-36434104
[233] https://malware.dontneedcoffee.com/2016/06/is-it-end-of-angler.html

Adobe Flash	CVE-2015-8651
Silverlight	CVE-2016-0034
Adobe Flash	CVE-2015-5560
Adobe Flash	CVE-2016-1001
Adobe Flash	CVE-2015-0359
Adobe Flash	CVE-2015-7645
Adobe Flash	CVE-2015-3090
Adobe Flash	CVE-2015-3113
Adobe Flash	CVE-2015-5119
Adobe Flash	CVE-2015-5122
Adobe Flash	CVE-2014-8439
Adobe Flash	CVE-2014-8440
Adobe Flash	CVE-2016-4117
Adobe Flash	CVE-2015-0311
Adobe Flash	CVE-2015-0313
Adobe Flash	CVE-2015-0336
Adobe Flash	CVE-2015-0310
Adobe Flash	CVE-2014-0497
Silverlight	CVE-2013-0074
Silverlight	CVE-2013-3896

Observed payloads delivered through the Angler exploit kit:

Ransomware: Teslacrypt, Torrentlocker, CryptoWall, Alpha Crypt ransomware, CryptXXX

Trojan: Kovter, Andromeda, Vawtrak, Poweliks, Dynamer, Trapwot, Graftor/Zbot, Bedep, Ursnif

5.2.2.7.3 Neutrino Exploit Kit

The Neutrino exploit kit was advertised in the underground forum in 2013. It initially started with exploits for vulnerabilities in the Java Runtime Environment (JRE), and later added support for exploiting vulnerabilities in the JScript and VBScript engines used in Internet Explorer and Adobe Flash Player.

Its campaigns were observed to involve compromising websites, typically WordPress, or malvertising, and injecting malicious iframes that loaded the Neutrino landing page.[234] Landing pages are hosted on randomly generated hosts using a domain generation algorithm (DGA), redirecting the victim to its payload. Neutrino operators also abused free domains registered inside the country code top-level domains (ccTLD) such as .top, .pw, .xyz, .ml, .space and others.[235]

Operators offered rent on a shared server with the following rates when it was first advertised in 2013:[236]

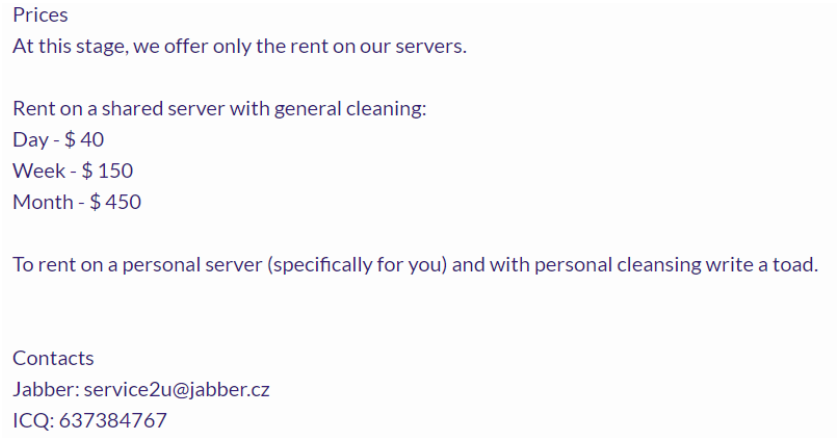


Figure 8: Neutrino exploit kit pricing 2013

In 2014, new pricing was advertised:[237]

[234] https://blog.talosintelligence.com/2016/09/shadowgate-takedown.html
[235] https://blog.talosintelligence.com/2016/09/shadowgate-takedown.html
[236] https://malware.dontneedcoffee.com/2013/03/hello-neutrino-just-one-more-exploit-kit.html
[237] https://malware.dontneedcoffee.com/2014/11/neutrino-come-back.html

[238]:

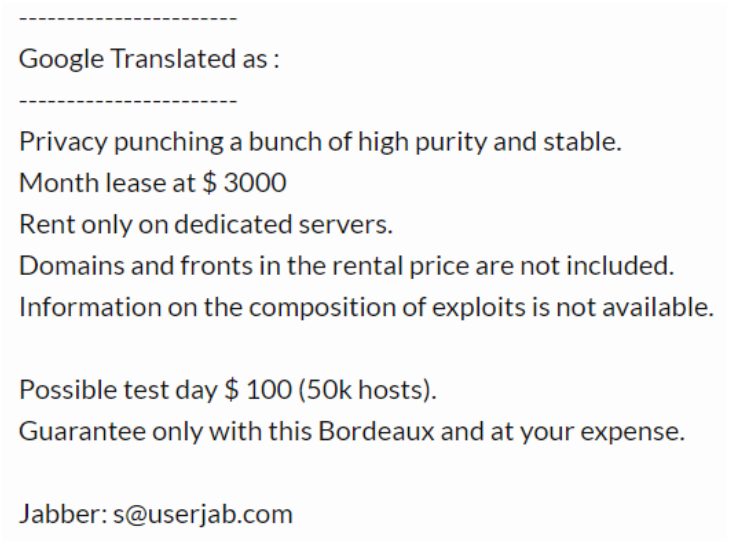


Figure 9: Neutrino exploit kit pricing 2014

From June until September 2016, it was found to be the most used by malvertising campaigns, suggesting it was the favourite kit for cyber-criminals at that time. In September 2016, its operators decided to go into "private mode", catering to a small number of selected customers. For months, Neutrino was still in operation and infecting users, but in a much smaller number. In June, F-Secure observed a significant drop in infection from its telemetry, while a researcher also claimed that the Neutrino owner said the exploit kit had stopped being profitable. This may be due to its exploits becoming outdated, and less effective in infecting users, a Kafeine researcher has explained.[239]

Summary of vulnerabilities exploited by the Neutrino exploit kit:[240]

Java	CVE-2012-1723
Java	CVE-2013-0431
Internet Explorer	CVE-2014-6332
Internet Explorer	CVE-2016-0189
Adobe Flash	CVE-2015-8651
Adobe Flash	CVE-2016-1019
Adobe Flash	CVE-2016-4117

[238] https://malware.dontneedcoffee.com/2014/11/neutrino-come-back.html
[239] https://www.bleepingcomputer.com/news/security/former-major-player-neutrino-exploit-kit-has-gone-dark/
[240] https://malware.dontneedcoffee.com/blog/

5.2.2.7.4 Nuclear Exploit Kit

The first version of the Nuclear exploit kit was distributed in 2009. In 2012, its second version, Nuclear Pack 2.0, was introduced, with advertised support for exploiting vulnerabilities in Acrobat Reader, Internet Explorer, JRE Trusted Method Chaining, and Oracle Java Rhino Script Engine.[241] It was one of the most prominent kits in 2015 and has since disappeared.[242]

Its initial pricing as advertised in 2012, ranges from 300 WMZ for a weekly "rental on server with full support" to monthly rental for 1600[243]. WMZ is a WebMoney Transfer unit which is tied to the US dollar value so the prices are equivalent amount in USD.

```
List price:
Month:
30k / day limit / 1 month - 400 wmz
50k / day limit / 1 month - 500 wmz
100k / day limit / 1 month - 800 wmz
200k / day limit / 1 month - 1200 wmz
300k / day limit / 1 month - 1600 wmz

Week 1:
50k / day limit / 1 week - 200 wmz
100k / day limit / 1 week - 300 wmz
200k / day limit / 1 week - 400 wmz
300k / day limit / 1 week - 500 wmz

2 weeks:
50k / day limit / 2 week - 300 wmz
100k / day limit / 2 week - 500 wmz
200k / day limit / 2 week - 700 wmz
300k / day limit / 2 week - 900 wmz

Screenshots: http://www.sendspace.com/file/9834dy

Contacts:
Support: nuc_support@thesecure.biz
```

Figure 10:Nuclear exploit kit pricing[244]

Nuclear was known to be responsible for large campaigns delivering Locky ransomware. In 2016, Checkpoint's research reported more than 140,000 computers affected by ransomware

[241] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/a-new-neighbor-in-town-the-nuclear-pack-v20-exploit-kit/
[242] https://www.f-secure.com/en/press/p/are-exploit-kits-doomed-new-f-secure-threat-report-says-yes
[243] https://pastebin.com/7zdwjv4j
[244] https://pastebin.com/7zdwjv4j

payloads in more than 200 countries,[245] and it was speculated that its operations accumulated revenue of approximately $100,000 a month.[246]

Its campaigns included compromising websites, as with other exploit kits. It refers users to a Traffic Distribution Service (TDS) that redirects them to Nuclear's landing page, where the exploit is served and subsequently delivers the malicious payload.[247]

In April 2016, Checkpoint researchers published a report and exposed its infrastructure, which probably led to disruption of its operations. At the end of April 2016, the Nuclear infrastructure ceased its operations, and stopped serving malicious content and responding to requests from their IP addresses. Kafeine, a French security researcher, also reported that Nuclear's activity stopped in the same month.[248]

Summary of vulnerabilities exploited by the Nuclear exploit kit:[249,250,251]

Adobe Flash	CVE-2014-0515
Active	CVE-2013-7331
Internet Explorer	CVE-2013-2551
Silverlight	CVE-2013-0074
Java	CVE-2012-0507
Adobe Reader	CVE-2010-0188
Jscript in IE	CVE-2015-2419
Adobe Flash	CVE-2015-5122
Adobe Flash	CVE-2015-7645
Adobe Flash	CVE-2016-1019
Internet Explorer	CVE-2014-6332

Observed Payloads delivered through Nuclear Exploit kit:
Ransomware: Locky, Teslacrypt, Cerber,
Trojans: Gootkit, Ursnif, Zeus, Vawtrak, Qadars, Boaxxe, Waldek-G, Coverton

[245] https://blog.checkpoint.com/wp-content/uploads/2016/04/Inside-Nuclear-1-2.pdf
[246]https://blog.checkpoint.com/2016/05/17/inside-nuclears-core-unraveling-a-ransomware-as-a-service-infrastructure/
[247] https://blog.checkpoint.com/wp-content/uploads/2016/04/Inside-Nuclear-1-2.pdf
[248] https://blog.checkpoint.com/2016/06/23/the-infamous-nuclear-exploit-kit-shuts-down/.
[249] https://malware.dontneedcoffee.com/blog/
[250] https://blog.checkpoint.com/wp-content/uploads/2016/04/Inside-Nuclear-1-2.pdf
[251] https://blog.talosintelligence.com/2014/10/evolution-of-nuclear-exploit-kit.html

5.2.2.7.5 Fallout Exploit kit

The Fallout exploit kit appeared in August 2018. It was believed to be an updated version of the Nuclear Pack, given its similarities as regards behaviour (code generation using html) and URL pattern.[252]

Since its discovery, it has been used by cyber-criminals to distribute several kinds of malware, including ransomware and potentially unwanted programs (PUA). Its campaigns involved malvertising targeting the Asia Pacific region, the Middle East and Southern Europe. It targets specific users by checking their browser profile: if the profile matches the targeted user, they are redirected to the exploit kit landing page. Fallout is able to exploit vulnerabilities in Adobe Flash and VBScript. Its URL pattern changes continuously to avoid intrusion detection by pattern recognition software.[253]

Summary of vulnerabilities exploited by the Fallout exploit kit:

VBScript	CVE-2018-8174
Adobe Flash	CVE-2018-4878
Adobe Flash	CVE-2018-15982

Observed payloads delivered through the Fallout exploit kit:

Ransomware: GandCrab, SAVEfiles
Trojan: CoalaBot, SmokeLoader, AZORult[254]
Others: PUA (Potentially Unwanted Application)

5.2.2.7.6 Magnitude Exploit Kit

The Magnitude exploit kit, aka as Popads, is one of the exploit kits that are still being used by threat actors at the time of this writing. It has been offered in underground forums since 2013. As regards Magnitude exploit kit's business model, it is not rented for weekly or monthly use like the other exploit kits. Instead, its customers are allowed to redirect traffic to the exploit kit, in exchange for directing 5-20% of their victims to the exploit kit author. The exploit kit author then infects those victims with his own malware, usually with CryptoWall ransomware in 2014, which demands about $400-500 in BTC per victim.[255]

[252] https://nao-sec.org/2018/09/hello-fallout-exploit-kit.html
[253] https://blog.morphisec.com/increasing-fallout-from-the-fallout-exploit-kit
[254] https://www.cybereason.com/blog/watch-where-you-browse-the-fallout-exploit-kit-stays-active

[255]https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/a-peek-into-the-lions-den-the-magnitude-aka-popads-exploit-kit/

It was used in large malvertising campaigns delivering several different types of malware,[256] including ransomware.[257] In 2014, attackers abused Yahoo's advertising network to redirect users to websites leading to Magnitude's landing page, which subsequently delivered different payloads.[258]

It also made headlines when it was used in an attack on the official PHP website, when the site was found to contain a modified JavaScript ("userprefs.js") that led users to Magnitude's landing page.[259]

In the later years, it became a private exploit kit, and the actors using it have changed targets, focusing on delivering ransomware to users from countries in the Asia Pacific region via malvertising. A report based on the Kaspersky Security Network shows that countries targeted in 2019 and 2020 were South Korea, Taiwan and Hong Kong. Activity from this exploit kit suggests that it is still actively being maintained and developed. It was found exploiting a vulnerability in a JScript engine, a legacy component of Internet Explorer (CVE-2019-1367), which was a zero-day exploit discovered in the wild. It is also known to use an elevation of privilege exploit for CVE-2018-8641, developed by a prolific exploit writer known as "Volodya", who was famous for selling zero-day exploits to both APT groups and criminals.[260]

Summary of vulnerabilities exploited by the Magnitude exploit kit:[261,262,263,264]

Adobe Flash	CVE-2015-8651
Adobe Flash	CVE-2016-1019
Adobe Flash	CVE-2016-4117
Jscript/VBScript in IE	CVE-2016-0189
VBScript	CVE-2018-8174
Adobe Flash	CVE-2018-4878
Adobe Flash	CVE-2015-3105
Adobe Flash	CVE-2015-3113

[256] https://www.malware-traffic-analysis.net/2014/04/14/index.html
[257] https://threatpost.com/malvertising-leads-to-magnitude-exploit-kit-ransomware-infection/112894/
[258] https://thehackernews.com/2014/01/yahoo-ad-network-abused-to-redirect.html
[259] https://blog.malwarebytes.com/threat-analysis/2013/10/php-hack-redirects-to-magnitude-exploit-kit/
[260] https://securelist.com/magnitude-exploit-kit-evolution/97436/
[261] https://malware.dontneedcoffee.com/blog/
[262] https://www.trendmicro.com/en_us/research/17/j/magnitude-exploit-kit-now-targeting-korea-with-magniber-ransomware.html
[263] https://securelist.com/magnitude-exploit-kit-evolution/97436/
[264]https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/a-peek-into-the-lions-den-the-magnitude-aka-popads-exploit-kit/

Jscript in IE	CVE-2015-2419
OpenType Font Driver	CVE-2015-2426
Adobe Flash	CVE-2015-7645
IE	CVE-2015-2413
Adobe Flash	CVE-2015-0311
Adobe Flash	CVE-2015-3090
Adobe Flash	CVE-2015-5119
Adobe Flash	CVE-2015-0336
IE	CVE-2013-2551
Adobe Flash	CVE-2015-5122
Adobe Flash	CVE-2015-0359
Jscript in IE	CVE-2019-1367
Win32k Elevation of Privilege	CVE-2018-8641
IE	CVE-2013-2551
Java	CVE-2013-2463
Java	CVE-2012-0507

Observed payloads delivered through the Magnitude exploit kit:

Ransomware: Locky, Cryptowall, CryptoDefense, Cerber, Magniber[265]
Trojans/Backdoors/InfoStealers: Neverquest, Alureon, Necurs, Nymaim, Simda, Tepfer, Vawtrak

5.2.2.7.7 RIG exploit kit

The RIG exploit kit was first seen in 2014 in the underground market, with initial rental prices ranging from $30/day to $500/month. In addition, the operators of Rig also have a reselling model, where a reseller can have their own admin panel that will allow their own customers to deploy their own campaigns. According to data collected from 2014 and 2015, based on the

[265] https://www.trendmicro.com/en_us/research/17/j/magnitude-exploit-kit-now-targeting-korea-with-magniber-ransomware.html

resellers and customers found, the RIG exploit kit could have been generating up to $90,000 per week during that time.[266]

Since its appearance, it has remained active and is being used by threat actors. According to a report from Sentinelone in 2019, its monthly subscription prices have changed, ranging from $700 to $2000 US.[267]

RIG campaigns, similarly to other exploit kits, involve compromising insecure websites by injecting malicious scripts into HTTP or PHP code on one of the pages. The injected code redirects visitors to the compromised website to the exploit kit page, serving the exploits and subsequently delivering malicious payloads. It was also known to frequently use domain shadowing, and as it evolved, it was found to be using IP addresses instead of URLs, and Base64-encoded strings instead of English words in the URL, to evade detection by security products.[268]

Summary of vulnerabilities exploited by the Rig exploit kit:[269,270,271]

Java	CVE-2012-0507
Java	CVE-2013-2465
IE	CVE-2013-2551
IE	CVE-2013-0322
Adobe Flash	CVE-2014-0497
Adobe Flash	CVE-2015-0311
Silverlight	CVE-2013-0074
IE	CVE-2014-6332

Observed payloads delivered through the Rig exploit kit:

Ransomware: CryptoShield 1.0, Spora, Revenge, PyCL, Matrix, GandCrab
Trojan/Backdoor/InfoStealer: Amadey, Clipboard Hijacker, Ramnit, Pony, AZORult, and Grobois

[266]https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/rig-exploit-kit-diving-deeper-into-the-infrastructure/
[267] https://labs.sentinelone.com/reversing-rig-exploit-kit-infection-chain-internals-exploits/
[268] https://cyware.com/news/dissecting-the-activities-and-capabilities-of-rig-exploit-kit-98d0a963
[269] http://www.kahusecurity.com/posts/rig_exploit_pack.html
[270]https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=7063a33f-41b9-41b2-8500-f32fa88c7cbb&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
[271] https://malware.dontneedcoffee.com/2015/01/cve-2015-0311-flash-up-to-1600287.html

5.2.2.8 Botnets

The first botnets were introduced in the IRC network in order to facilitate the administration of IRC channels (Cooke et al., 2005). IRC administrators were able to issue commands from their personal workstations and the IRC servers would execute these commands on the IRC network. These robot servers were referred to as bots and the network of bots as a botnet. In the following years, botnets were used for unethical purposes without the knowledge of the IRC users. Today, botnets can infect any kind of computer (not only through the IRC network) and are used for illegal purposes, such as DDoS, sending spam emails, spreading of malware, and theft of credentials and credit card data (Hyslip, 2020). We consider botnets and their operations as a driver for cybercrime.

Technically, developing and operating a botnet is challenging and can be done only by experts. The Cybercrime-as-a-Service model (see Section 6) has helped make this technology easier for public use and maintenance by providing services such as purchasing or renting a complete botnet. Nontechnical criminals can now use botnets, even if they could not before.

When a botnet is rented, the vendor provides the IP address of the C&C interface and the credentials to be used. Then the buyer visits the website (probably served from deep web via TOR) and gains access to use captured credit cards, perform DDoS attacks and tailor spam messages.

Another scenario, for more technically experienced criminals, is to purchase the botnet infrastructure (C&C software, malware to infect computers, etc.) and then set up their own botnet. An advantage of this approach is that the seller will not know the details of the attack. Another advantage is that in most countries creating and selling such type of software is not illegal, in contrast to selling a complete botnet, which is probably an illegal action. In this case, the purchaser also needs to get a bulletproof hosting service (see Section 6.2) to install the C&C server.

Below is the list of the most notorious botnets to date.[272] Most of them are now or were in the past available for sale or rent and have been used by criminals for various malicious operations over the last years:

- EarthLink Spammer (2000): Over 1.25 million malicious phishing emails were sent by this botnet over a year in order to collect credit card information from the victims. The botnet had also downloaded other viruses to the victims' computers that remotely fed the attacker with more information.
- Cutwail (2007): This botnet remains active and available for rent today, even though the authorities attempted to take it down in 2014. Over 2 million infected Windows systems sent billions of spam messages every day. In 2009 specifically, this botnet contributed to the 46.5% of the entire world's spam volume.
- Storm (2007): One of the first peer-to-peer botnets that can be controlled from several different servers and has the ability to update its code. Storm is not contained in the spam message itself, but in malicious websites where the recipient visits via the email and downloads the malware. It could be rented out on the Dark Web and it was involved

[272] https://www.whiteops.com/blog/9-of-the-most-notable-botnets

in various malicious activities from DDoS attacks to identity theft. Most of the servers were shut down in 2008, so it is not very active these days.

- Grum (2008): A pharmaceutical spammer bot that was able to send 39.9 billion messages per day, or 18% of the world's spam in 2009. Security researchers helped authorities to locate and take down Grum in 2012.
- Kraken (2008): A very powerful botnet that infected 10% of all Fortune 500 companies. About half a million bots could send as many as 600,000 emails per day. Its evasion techniques made Kraken invisible to antimalware software.
- Mariposa (2008): It was created with software called Butterfly Flooder from which it got its name, which means "butterfly" in Spanish. Mariposa infected over 10 million computers for two years in more than 150 countries through various means and methods, but mainly with malvertising. Until its end, after the authorities discovered records of people who had rented it, the botnet had stolen millions of US dollars by getting credit card numbers and bank account credentials from the victims.
- Conficker (2008). It is a network worm also known as Downadup, Downup, or Kido. Beginning in late 2008, it infected millions of machines to form a massive botnet. It exploited the Windows Vulnerability in Server Service (MS08-067) and used heavy server-side polymorphism to make detection difficult. To fight against the big outbreak, Microsoft formed the Conficker Working group and offered a $250,000 bounty for information leading to the arrest of the worm creators. As it was spreading in the wild, the threat actors were releasing new versions of the worm to increase defences, and added "peer-to-peer" capabilities that allowed infected computers to communicate over networks so they could be updated without the need to reach any web domains. Later versions used to install a "scareware" program that imitated anti-virus software to extort money from users. It was suspected that this version of Conficker was from a different group of actors who rented out the botnet. Essentially, Conficker was initially designed to spread to as many machines as possible, creating a massive botnet of infected machines that could be used for other malicious activities such as spreading spam, scareware and various payloads. In the observed outbreak, it was only seen to deliver scareware once.[273]
- Methbot (2016): The operators of this botnet first acquired thousands of IP addresses and created more than 6000 domains and 250,267 distinct URLs that appeared to belong to real big-name publishers. Then, they got advertisers to bid on them and after that they put their bots to mimic the behaviour of a human that uses a real browser and consumes the advertisements. The group of Russian criminals who created the botnet were earning between $3 to $5 million US daily from the advertising market. Methbot was discovered and uprooted by White Ops in 2015.
- Mirai (2006): Mirai was the first wide scale botnet discovered that targeted vulnerable IoT devices and used them to launch DDoS attacks. Mirai identifies IoT devices that use "easy-to-guess" passwords. The initial access is achieved by logging into devices with default factory usernames and passwords. These are stored in a table of 60 different combinations; after a successful login the device is infected with Mirai mawlare. Mirai

[273] https://blog.f-secure.com/what-weve-learned-from-10-years-of-the-conficker-mystery/

was prevalent malware, with about 600,000 devices infected in its prime. Mirai had infected many different IoT devices, such as IP cameras, home routers and video players. Mirai's source code was later open-sourced and made public in the "Hackforums" community. Since the code became public, the different techniques implemented have been adopted in other types of malware and enabled cybercriminals with even modest information technology skills to develop a botnet with attack potential whilst expending little effort.

- 3ve (2018): 3ve utilised the malware packages Boaxxe and Kovter to infect a network of PCs and then generate fake clicks on online advertisements. The clicks performed through fake websites which hosted the ads and criminals were paid the ad revenue. It infected around 1.7 million computers and a large number of servers. About $30 million US was stolen over the time the botnet was in use. Google, White Ops, and other tech companies, including Adobe, the Trade Desk, Amazon Advertising, Oath, Malwarebytes, ESET, Proofpoint, Symantec, F-Secure, McAfee, and Trend Micro coordinated to shut down 3ve's operations.

5.3 Exploitation

In cybersecurity, the word exploit is used to describe a piece of code that takes advantage of vulnerabilities in applications, networks, operating systems or hardware to cause unintended or unanticipated behaviour.
Exploits are used in several ways by cybercriminals: as entry points into a victim's computer/network, to sabotage, to escalate privileges from a local user to admin, or to pivot to other machines in the victim's network. The method used depends on the goal of the cybercriminal.

5.3.1 Trends in Exploitation

To demonstrate the trends in exploitation, some of the major events in cybersecurity throughout the years are detailed below. This is not a fully comprehensive review, but rather picks up the major trends to convey how cybercriminals have approached exploitation over time. Here, the focus is primarily on PC malware.

5.3.1.1 Major events

We examine events during the last 2 decades that were significant in terms of either their impact, the losses caused, or their unprecedented nature that shaped subsequent exploits.

5.3.1.1.1 2000 - ILOVEYOU worm

In May 2000, Onel De Guzman, a college student in the Philippines, released one of the most damaging worms ever, with damage estimates floating around $5-10 billion US.[274] It spread across the whole world, impacting millions. The purpose, De Guzman said, was to steal other

[274]https://www.forbes.com/sites/daveywinder/2020/05/04/this-20-year-old-virus-infected-50-million-windows-computers-in-10-days-why-the-iloveyou-pandemic-matters-in-2020/?sh=3c9c24683c7c

users' passwords so that he could use them to access the internet without paying. However, the worm also inflicted damage on the victim's machine, overwriting random types of files and propagating by sending a copy of itself to all addresses in their Outlook Windows Address Book.

The virus arrived as an email attachment sent to victims, with the filename "LOVE-LETTER-FOR-YOU.TXT.vbs". The double extension duped users into thinking it was a txt file, and a windows 95 'bug' meant that once clicked the malicious vbs script ran.

This exemplifies that in the early days of the internet, individual users could cause widespread harm, since the technologies were immature, with many not utilising spam filters to filter such a worm or antivirus solutions to detect the payload.

5.3.1.1.2 2003 - SQL Slammer

In 2002, a vulnerability researcher, David Litchfield, responsibly disclosed to Microsoft several vulnerabilities affecting the Microsoft SQL Server software. Microsoft fixed these and released a patch. Six months later Litchfield gave a talk at Blackhat[275], presenting his work and including a PoC of one of the vulnerabilities, a stack buffer overflow. A month later, on 25 January 2003, a malicious actor released a computer worm named SQL slammer utilising the PoC.

SQL slammer worked by infecting a vulnerable SQL server, then propagating the exploit to other hosts, in turn infecting them. While not malicious to the hosts, SQL slammer caused a spike in traffic from the cascade of servers infecting each other, and soon overwhelmed the routers and the internet traffic, causing a slowdown of the internet. Within 10 minutes of SQL slammer being released, an estimated 75,000 victims were affected, climbing afterwards to a total of around 250,000 victims.[276]

This case provided two big lessons for the security industry: that users should patch their software, and that security researchers should be very careful in releasing PoCs. Litchfield in an interview notes:

"One positive aspect of Slammer was the effect it had on patching – prior to Slammer I'd guesstimate, from the results of penetration tests and so on, that 9 out of 10 SQL Servers were unpatched. Immediately after Slammer this reversed leaving 1 out of 10 unpatched".[277]

5.3.1.1.3 2010 - Stuxnet

Stuxnet is a malicious computer worm, developed by the US and Israel to target the Iranian nuclear enrichment program. It was discovered in 2010 and is believed to have been developed since at least 2005.[278] The malware targeted the enrichment centrifuges, causing them to tear themselves apart and making it appear as if the centrifuges were faulty. For many years the Iranians discarded the centrifuges, believing they were faulty.

It was a sophisticated targeted attack, with the worm programmed to avoid running outside of the target in Iran, and featured four zero days. It was transferred to the air-gapped nuclear plant computer systems through a USB stick.

[275] https://www.blackhat.com/html/bh-asia-02/bh-asia-02-speakers.html
[276] https://www.welivesecurity.com/2016/09/30/flashback-friday-sql-slammer/
[277] https://threatpost.com/inside-story-sql-slammer-102010/74589/
[278] https://www.reuters.com/article/us-cyberwar-stuxnet-idUSBRE91P0PP20130226

This attack shocked the cybersecurity industry and the world, it was the first example of a nation-state cyberweapon on display and the malware itself was incredibly impressive, unlike anything researchers had seen before. It displayed the power nation-states have in cybersecurity and the zero days they harbour.

5.3.1.1.4 2010 - Blackhole EK

The Blackhole exploit kit first appeared in 2010. By 2012 it was the most prevalent exploit kit in use, accounting for a third of the exploit kit detections at F-Secure. Cybercriminals were able to rent the exploit kit; the reported price was $500 to $700 each month.[279] The cybercriminals would then host the kit on a compromised site and wait for users to visit it and become infected. Other infection vectors were to utilise the kit through SEO poisoning and email spam. The exploits Blackhole primarily targeted were browser plugins, such as Java, Adobe Reader and Adobe Flash Player.

The relative immaturity of browsers and web technology compared to today meant the exploit kits were extremely successful. Blackhole succeeded for so long as the top kit because the developers reliably incorporated the latest CVEs very soon after they were released, catching victims who were yet to upgrade their Flash or Java version, for example. The developers were reported to source the exploits by purchasing from cybercriminal exploit developers.[280]

Because of its devastating success, Blackhole became the subject of law enforcement agencies, and in October 2013 the group was arrested. Immediately, AV companies, including F-Secure, saw the exploit kit fade away and instead be replaced with other kits, with Angler taking the helm.

5.3.1.1.5 2012 - Flashback OSX

In 2012, big malware outbreaks on the Mac OS X were unheard of and Flashback was the first such outbreak on a massive scale, reportedly infecting more than 600,000 Macs around the world.[281] It was distributed via drive-by downloads, where users visit legitimate but compromised websites. These websites were altered to redirect visiting users to malicious sites hosting the actual malware. The trojan exploited the then-unpatched CVE-2012-0507 vulnerability in Java, and on success the malware modified the contents of certain web pages displayed by web browsers.

While the vulnerability Flashback was exploiting had been patched by Oracle (Developer of Java) and so was closed for Windows hosts, Apple was responsible for Java updates for OSX and had not released a patch for Mac endpoints. This led to the unfortunate situation where thousands of OSX Java users were vulnerable to CVE-2012-0507.

This outbreak highlighted that the popular belief at the time of the Mac's "immunity" to malware was unfounded and showed that Macs, just like other platforms, would benefit from defensive cyber security solutions. This also prompted Apple to improve their security,

[279] https://krebsonsecurity.com/2016/04/blackhole-exploit-kit-author-gets-8-years/
[280] https://krebsonsecurity.com/2016/04/blackhole-exploit-kit-author-gets-8-years/
[281]https://arstechnica.com/gadgets/2012/04/flashback-trojan-reportedly-controls-half-a-million-macs-and-counting/

including a feature that automatically deactivated the Java browser plugin and Java Web Start after 35 days of inactivity.[282]

For Flashback, the trend of cybercriminals targeting new platforms with many users and pouncing on unpatched vulnerabilities was evident.

5.3.1.1.6 2012 - Flame

The Flame malware was a similar case to Stuxnet, believed to be developed by western intelligence agencies and with researchers touting it as the most sophisticated malware ever found,[283] once again reminding everyone that nation-state capabilities in cyber security are extremely powerful and far beyond average cybercriminals. Similarly, it also showed that nation-state malware is not widespread, but rather highly targeted. In the case of Flame, the target was a limited number of computers in the Middle East with the malware able to record audio, screenshots, keyboard activity and network traffic, and to extract documents.

5.3.1.1.7 2013 - Angler EK

With the demise of BlackHole EK, Angler took the leading place,[284] deploying similar tactics to Blackhole EK. During this time period, exploit kits continued to be incredibly popular with cybercriminals. Angler EK remained at the top, until in 2016 they were also targeted and taken down by law enforcement agencies.[285]

5.3.1.1.8 2014 - Heartbleed, Shellshock

In 2014, there were two core pieces of software, the OpenSSL cryptographic software library and the Unix bash shell, which had significant vulnerabilities discovered and subsequently exploited.

Heartbleed refers to the OpenSSL vulnerability for the SSL/TLS encryption that is integrated into many popular software packages, including open source web servers Apache and nginx. At the time, the market share of just those two on the Internet was reported to be over two thirds.[286] On 7th April, the day of the public disclosure, a patch was released for Heartbleed. The Tor project noted: “If you need strong anonymity or privacy on the Internet, you might want to stay away from the Internet entirely for the next few days while things settle”, and the race for system administrators to incorporate the patch was on.

One month later, in May 2014, 1.5% of the 800,000 most popular TLS-enabled websites were still vulnerable to Heartbleed,[287] and 5 years later, in 2019, Shodan reported that 91,063 devices were still vulnerable.[288] The vulnerability was immediately exploited by cybercriminals.[289]

Shellshock refers to the vulnerabilities found in the Unix bash shell, allowing attackers unauthorised access to and abilities to execute any code of their choice on many public Internet-facing services. This ability, to execute code of an attacker’s choice remotely, is known as

[282] https://support.apple.com/en-gb/HT202455
[283] https://www.webcitation.org/682bQ4f6J?url=http://www.crysys.hu/skywiper/skywiper.pdf
[284] https://news.sophos.com/en-us/2015/07/21/a-closer-look-at-the-angler-exploit-kit/
[285] https://threatpost.com/inside-the-demise-of-the-angler-exploit-kit/120222/
[286] https://news.netcraft.com/archives/2014/04/02/april-2014-web-server-survey.html
[287] https://www.theregister.com/2014/05/20/heartbleed_still_prevalent/
[288] https://web.archive.org/web/20190711082042/https://www.shodan.io/report/0Wew7Zq7
[289] https://time.com/3148773/report-devastating-heartbleed-flaw-was-used-in-hospital-hack/

remote code execution (RCE). The bug was responsibly disclosed by a security researcher, and soon a patch was released and publicly disclosed. Immediately, cybercriminals raced to exploit this just hours later, compromising servers and building up botnets.[290,291]

Both of these critical bugs demonstrated that core libraries we heavily depend on will be exploited, and that ensuring that software and services are quickly and easily patchable is the only way to defend against cybercriminals who can operate at a moment's notice.

5.3.1.1.9 2017 - CCleaner supply chain

CCleaner is a piece of software meant to "clean" computers by getting rid of temporary files and invalid Windows registry keys. In 2017, it had been downloaded more than 2 billion times. However, in rather iconic circumstances, the piece of software meant to clean systems also infected users when attackers compromised the CClearer's build environment—a supply chain attack. The parent company of CCleaner, Avast Piriform, then distributed the CCleaner malicious software unknowingly to approximately 2.27 million users.[292] The malicious part of code was collecting sensitive data and relaying it back to the attackers.

This was a widespread attack, and not the first nor the last supply chain attack (see section 5.7). Supply chain attacks prove just how critical build systems are for software. Their compromise is of very high value to cybercriminals, since the resulting software is immediately trusted by users.

5.3.1.1.10 2017 - Wannacry

In May 2017, the Wannacry ransomware cryptoworm ripped through the world, devastating many organisations around the world, most notably the United Kingdom's healthcare system, the NHS. The malware targeted older Windows systems using an exploit that was stolen from the NSA and released publicly, named EternalBlue. Microsoft had released patches for this vulnerability after the NSA leak; however, many system administrators had yet to patch their systems. There was uproar in this case towards the NSA who had harboured this zero day exploit and likely used it offensively without disclosing it to Microsoft.

The ransomware crypto worm exploits the unpatched SMB protocol on the victim, checks if the kill switch domain exists or not, then if not it proceeds to encrypt the computer's data before spreading to other vulnerable computers on the network. The malware displays on the victim's machine that the files are encrypted and demands a ransom payment to a Bitcoin address to decrypt the documents and restore use. Fortunately, a security researcher registered the kill switch domain and effectively stopped the progress of the attack.

This case showed the rise in the use of ransomware, the harbouring of zero day exploits by nation states and the continued failure of system administrators to patch their systems with security updates. The cyber criminals took advantage, using the work of the NSA.

5.3.1.1.11 2017 - NotPetya

A month after the Wannacry attacks, NotPetya, a variant of the previous Petya encrypting malware, hit the scene, causing more widespread destruction. Similar to Wannacry, it used the EternalBlue exploit, but NotPetya was entirely destructive, irreversibly encrypting computers'

[290] https://www.itnews.com.au/news/first-shellshock-botnet-attacks-akamai-us-dod-networks-396197
[291] https://www.wired.com/2014/09/hackers-already-using-shellshock-bug-create-botnets-ddos-attacks/
[292] https://www.theverge.com/2017/9/18/16325202/ccleaner-hack-malware-security

master boot records. The US estimated NotPetya caused $10 billion US in damages.[293] The malware has been accredited to the Russia Sandworm unit and was a highly sophisticated operation meant to target Ukraine.

The lesson was that cyber criminals will continue taking advantage of "old" exploits, since there will always be victims without a patch, even when system administrators have been given several harsh warnings.

5.3.1.1.12 2017 - Coinhive

From 2017 to 2019, Coinhive featured as one of the top malicious threats to web users. Coinhive was a cryptocurrency service, where mining scripts could be inserted into webpages to mine the anonymous focused Monero cryptocurrency. This meant that, when a user visited such a site with the Coinhive feature, the user's computer would start mining cryptocurrency for whoever added the feature. The purpose of this service was to replace website ads as a way for the host to make money. The cybercriminals exploited websites or advertisements to be shown on webpages, placing the Coinhive scripts in them, resulting in visitors to the sites unknowingly mining cryptocurrency for cybercriminals.

Coinhive was found in websites such as the Los Angeles Times, Youtube Advertisements, Blackberry and many more. Publicwww, which indexes the source code of websites, showed there were nearly 32,000 web sites currently running Coinhive's JavaScript miner code.[294] With the widespread malicious use of Coinhive, the creators shut down the service in 2019.[295]

While these public-facing services were exploited in a conventional way, the abuse of the Coinhive mining service for cybercriminal activities was novel and particularly widespread. This also paved the way for more interest directed towards malicious coin mining.

Cybercriminals continue to mine cryptocurrencies at the victims expense, especially now with the heavy adoption of cloud computing infrastructure, where sysadmins may not pay as much attention to the bandwidth and resource usage reports of compromised servers—normally the finance department discovers the cases when cloud costs skyrocket.

5.3.1.1.13 2017 - Emotet MaaS

Emotet was first identified in 2014, starting as a banking trojan before evolving into Malware as a Service (MaaS) in 2017. The MaaS positioned Emotet to act as a packing and delivery service for other malware, such as Trickbot, Qakbot, Dridex. Emotet is covered here, since it was highly successful as such a service between 2017 and 2021, featuring as a top prevalent threat, so much so that it prompted government agencies to launch a big shutdown in 2021.[296]

Emotet was spread via email spam with malicious Microsoft document attachments, luring victims into opening them and executing malicious macro code. Emotet is a great example of

[293]https://web.archive.org/web/*/https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/
[294] https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/
[295]https://www.theverge.com/2019/2/28/18244636/coinhive-cryptojacking-cryptocurrency-mining-shut-down-monero-date
[296]https://www.europol.europa.eu/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action

the recent years of such tactics for cybercriminals, exploiting macros in word documents and continuously evolving their approach to avoid detection.

5.3.1.1.14 2020 - Solarwinds supply chain

At the end of 2020, a devastating cyberattack aimed at US government agencies and Fortune 500 companies came to light. The White House attributed the hack to Russia.[297] The hack itself was a sophisticated supply chain attack on the company Solarwinds Orion product, an IT monitoring and management software. The attackers injected malicious code into an update spread to 18,000 users, creating a backdoor into the victims' servers.

US agencies, parts of the Pentagon, Department of Homeland Security, State Department, Department of Energy, National Nuclear Security Administration and more were attacked, as well as private companies, such as Microsoft, Deloitte, Cisco and Intel.[298] Organisations had been affected many months prior to the finding in December 2020 by Fireeye, and with the sophisticated actors cleaning up afterwards it remained hard to identify which companies were infiltrated.

This case further emphasises the high value vector of supply chain attacks for cybercriminals, in this case the infiltration of Solarwinds release management infrastructure.

5.3.1.1.15 2021 - Microsoft Exchange Server hack

In March 2021, four zero day vulnerabilities were reported to be actively exploited by cybercriminals. China was later implicated as the primary threat actor.[299] The zero days and the PoC code were responsibly disclosed in January by a security researcher and the later exploitation was found to be utilising very similar PoC code.[300] Microsoft released an out-of-band patch in March. However, as appears to be the pattern in these attacks the patches were not applied soon enough, with 125,000 unpatched servers worldwide as of March 9,[301] one week after the patch release date.

5.3.1.2 Top exploited vulnerabilities 2016-19

In May 2020, US governmental agencies posted a public alert of the top 10 routinely exploited vulnerabilities by foreign cyber actors between 2016 and 2019.[302] This study of highly exploited vulnerabilities in recent years shows that cybercriminals have been heavily focusing on Microsoft Office. The exploits either start off being developed and exploited by highly sophisticated actors, such as those known as Advanced Persistent Threat (APT) groups, or are disclosed by security researchers, only then to be released publicly online. Once online, even though the patches are often available, users still take a long time to patch, and during this time more and more cyber criminals could pick up these exploits and utilise them.

[297] https://www.whitehouse.gov/briefing-room/press-briefings/2021/04/15/background-press-call-by-senior-administration-officials-on-russia/
[298] https://www.wsj.com/articles/solarwinds-hack-victims-from-tech-companies-to-a-hospital-and-university-11608548402?mod=djemalertNEWS
[299] https://www.ncsc.gov.uk/news/uk-allies-hold-chinese-state-responsible-for-pervasive-pattern-of-hacking
[300] https://proxylogon.com/
[301] https://unit42.paloaltonetworks.com/remediation-steps-for-the-microsoft-exchange-server-vulnerabilities/
[302] https://us-cert.cisa.gov/ncas/alerts/aa20-133a

The following list contains those 10 mentioned in the report, in order of descending popularity, along with some further notes about the particular exploit and how it was discovered.

1. CVE-2017-11882 - Buffer overflow in the Microsoft Office equation editor dating back to a component used since November 9, 2000. The vulnerability was reported to Microsoft by Russian cybersecurity startup Embedi[303] on 03/08/2017 and patched on 14/11/2017. After the patch, exploits were widely available on sites such as Github and there was a component in Metasploit.[304]
2. CVE-2017-0199 - Microsoft Office vulnerability in the OLElink object, allowing a malicious RTF file to make an http request and in response execute HTA code. FireEye discovered malware exploiting this vulnerability in the wild. Several days after the release of this news, researchers had found the malware in question and reverse engineered the exploit in use and published the exploit as a free metasploit module.[305]
3. CVE-2017-5638 - Apache Struts web framework vulnerability targeting the Jakarta Multipart parser allowing remote code execution.[306] A researcher found and disclosed the vulnerability, it was patched and an advisory was sent out. A few hours after the advisory, exploit code was found available online by researchers who had crafted the exploit by diffing the patch.
4. CVE-2012-0158 - Buffer overflow in the ListView/TreeView ActiveX controls in the MSCOMCTL.OCX library.[307] The exploit for this vulnerability was seen in the wild shortly after the patch and PoCs were available online.
5. CVE-2019-0604 - Deserialisation vulnerability in Microsoft Sharepoint servers. Discovered by a researcher who reported it to Zero Day Initiative and seen in the wild soon after the patch,[308] with PoCs available online.
6. CVE-2017-0143 - Crafted packets targeting the SMBv1 server in Microsoft Windows, allowing for arbitrary code execution.[309] This vulnerability was part of the NSA exploit and hacking tools released by the Shadow Brokers. After the release it was utilised widely, even after the patch, most infamously in the Wannacry Ransomware.
7. CVE-2018-4878 - Adobe Flash Player vulnerable ActiveX object allowing RCE, seen used through Microsoft Excel. The exploit was seen in the wild by South Korea Agency KISA, believed to be used by North Korea hackers.[310]
8. CVE-2017-8759 - Microsoft Office RTF document vulnerability in the SOAP WSDL parser allowing code injection. FireEye discovered this in the wild to distribute FINSPY

[303]http://web.archive.org/web/20180811110001/https://embedi.com/blog/skeleton-closet-ms-office-vulnerability-you-didnt-know-about/
[304] https://unit42.paloaltonetworks.com/unit42-analysis-of-cve-2017-11882-exploit-in-the-wild/
[305] https://www.exploit-db.com/exploits/41934
[306]https://www.trendmicro.com/en_us/research/17/c/cve-2017-5638-apache-struts-vulnerability-remote-code-execution.html
[307] https://securelist.com/the-curious-case-of-a-cve-2012-0158-exploit/37158/
[308]https://www.zerodayinitiative.com/blog/2019/3/13/cve-2019-0604-details-of-a-microsoft-sharepoint-rce-vulnerability
[309] https://nvd.nist.gov/vuln/detail/cve-2017-0143
[310]https://www.trendmicro.com/vinfo/us/security/news/vulnerabilities-and-exploits/north-korean-hackers-allegedly-exploit-adobe-flash-player-vulnerability-cve-2018-4878-against-south-korean-targets

malware.[311] Shortly after the announcement and patch, exploit PoCs could be found freely online.[312]

9. CVE-2015-1641 - Microsoft Office Memory Corruption Vulnerability seen being exploited in the wild.[313] After the patch, exploits were available online.
10. CVE-2018-7600 - Insufficient input validation on the Drupal 7 Form API allows code execution on servers running Drupal.[314] The Drupal Core Security team released an advisory to upgrade and apply the Drupal patch, shortly after researchers diffed the patch and exploit code was available freely online.

5.3.2 Acquisition of exploits

Highly sophisticated attackers, such as APT groups, acquire exploits by discovering vulnerabilities themselves through research, purchasing through zero-day brokers such as Zerodium or purchasing on the Dark Web. Zerodium acquires these exploits for prices ranging from tens of thousands to millions of US dollars, and so one can imagine that the purchase price from Zerodium would be even higher. This means they are out of reach of most common cybercriminals.

Once the techniques of highly sophisticated actors are discovered or a patch has been released for a vulnerability, researchers quickly reverse the malware and exploits, releasing the exploits as free PoCs online or selling them on the Dark Web.

For the common cybercriminal, the speed of exploiting these new vulnerabilities does matter to a certain extent, as they race to exploit the unpatched users; however, many of the targets are slow to patch, as evidenced by the fact that in the top 10 exploited vulnerabilities for 2016-2019 we see CVEs from 2012 and 2015.

5.3.3 Summary and the future of exploitation

The chapter started in the 2000s with the ILOVEYOU worm and SQL slammer. Both were worms and demonstrated that, in those days with many users not utilising spam filters and antivirus solutions, worms were able to spread easily. Lessons were learned, particularly better spam filtering from the ILOVEYOU case and patch policies from SQL Slammer.

In 2010 Stuxnet was discovered, and this provided a shock to the capabilities of nation states, with the use of four zero-days and a highly sophisticated operation. This trend has continued, with APTs continuing to discover and purchase zero-days and evade the defensive technologies. Simply put, defending against APT cybercriminals is extremely hard, nearly impossible. Further examples covered above have been Flame, Solarwinds and Microsoft Exchange servers.

In 2012 Flashback OSX malware hit the scene, infecting a sizable proportion of Macs because Apple had not patched Java for their users. It broke down the common misconception that Macs were “immune” from malware and prompted Apple to seriously consider and improve their

[311] https://www.fireeye.com/blog/threat-research/2017/09/zero-day-used-to-distribute-finspy.html
[312] https://github.com/bhdresh/CVE-2017-8759
[313] https://docs.microsoft.com/en-us/security-updates/securitybulletins/2015/ms15-033
[314] https://unit42.paloaltonetworks.com/unit42-exploit-wild-drupalgeddon2-analysis-cve-2018-7600/

security. Apple products still do, however, continue to be misclassified as "immune" to malware: this is false, and the reason we do not see cybercriminals exploit Mac OSX more is that the high value targets, usually large organisations and businesses, use Windows.

The Blackhole exploit kit featured highly in 2012, and was arguably the most prevalent threat for users with its very high success rate and ease of use for cybercriminals. These exploit kits primarily targeted browsers, with Flash, Java and other zero days in browsers being continuously discovered and packaged into the exploit kits. This attracted the attention of law enforcement agencies, which took down Blackhole in 2013. Subsequently, Angler EK took the leading place before they too were taken down in 2016. The use of exploit kits after 2016 declined significantly as a result of improved browser security, the move away from Flash in browsers, fewer exploits found in web technologies such as Java, and law enforcement agencies cracking down on the cybercriminal groups.

With exploit kits in decline the common cybercriminals returned to the previous successful trend of spam distribution of malware. The primary vector was Microsoft office documents, exploited by specially crafted documents utilising social engineering and the powerful use of macros in a malicious way. Evidence from the US agencies confirmed this, with the top 3 most exploited vulnerabilities they saw between 2016-2019 concerning Microsoft Office. Emotet was the most prevalent family exploiting this vector until their take down in 2021; however, many other families continue to use it successfully.

Other patterns seen were the discoveries now and again in fundamental technologies such as Heartbleed and Shellshock in 2014. Despite the developers releasing patches promptly, users continue to lag in applying these and so cybercriminals rushed to exploit them. This is perhaps the most important trend: the fact that prevalent vulnerabilities exploited by common cyber criminals can already have a patch available but users are still vulnerable as they do not patch their systems promptly enough. This became evident with the Wannacry and NotPetya attacks in 2017, both targeting servers running outdated SMB services.

Wannacry and NotPetya were high profile ransomware cases, which has been a common trend—from 2016 the number of ransomware families has grown greatly. This technique has been extremely successful for cybercriminals and will continue to be with the utilisation of cryptocurrency to collect payment, which is difficult to trace.

The rise and effectiveness in supply chain attacks were seen in the CCleaner and Solarwinds cases. Both seem to have been carried out by APT groups, which shows this is a complex method to exploit; however, it is an extremely effective method and one that can help cyber criminals evade detection.

Another area of continued exploitation by cybercriminals is using victims' resources to mine cryptocurrency, with Coinhive being the most prevalent case here. Coinhive allowed cybercriminals to harvest the Monero cryptocurrency from unsuspecting users when they visited compromised sites. However, more common malware families have also incorporated mining functionality to begin after a standard initial infection of a victim's device.[315]

For the future of exploitation, the use of spam Microsoft office documents will likely remain the primary vector for the common cybercriminal. Other vectors will be the continued fast

[315]https://www.trendmicro.com/vinfo/de/security/news/cybercrime-and-digital-threats/security-101-the-impact-of-cryptocurrency-mining-malware

exploitation of vulnerabilities that are released and patched, where cyber criminals will purchase or pick up PoC exploits, or even develop them themselves through patch diffing. This method will always be seen, since devices are not patched soon enough after they are released. On the APT side we can expect to see more zero-day and supply chain attacks, where it will prove hard for defenders to detect them.

5.4 Emerging attacks on IoT and CPS

As described previously, the prevalence of IoT devices is ever increasing, resulting in impactful and damaging attacks.

We now enumerate and describe a few attacks on both IoT and CPS that have had deep impacts as well as promoting further malicious attacks:

- **Mirai variants/dictionary attacks** - Mirai was closely followed by numerous other attacks on IoT devices, typically, but not limited to IP cameras, by brute forcing their telnet passwords. Botnets such as Satori,[316] were built on top of Mirai by extending the range of "password brute forcing" to non-telnet ports, and in the process making large-scale DDoS attacks common. Similarly, the BrickerBot malware[317] also gains unauthorised access to an IoT device by employing dictionary attacks on vulnerable IoT devices. However, instead of exploiting the devices for further DDoS attacks, BrickerBot executes a series of Linux commands to permanently brick those devices, making it a devastating PDoS attack.
- **Other vulnerabilities** - After dictionary attacks/password brute-forcing became commonplace, attackers soon expanded their repertoire to exploit other vulnerabilities in IoT devices. Persirai,[318] for example, exploited a vulnerability that exposed device credentials by allowing unauthenticated access to a .ini file on the device. A simple HTTP request to a URL of the type *http://<ip_address>/path/system.ini*, without any authentication, would fetch the system.ini file. This file contains the login credentials for the device in plaintext, which can be then misused by attackers. Meanwhile, Hakai (Tambe, 2019) and IoTReaper malware[319] extended Mirai by packing exploits for several vulnerabilities, thereby making those more potent. Unlike Mirai, which scanned only for telnet port access with a dictionary of default credentials, IoTReaper introduced more intelligence in the attack scripts by including exploits for as many as 9 previously known vulnerabilities. Such vulnerabilities encompassed devices from various brands, such as D-Link, TP-Link, AVTech, Netgear, etc., allowing attackers to exploit a plethora of devices.
- **Smart homes** - Apart from Mirai-styled large-scale attacks, security incidents involving various breaches in IoT devices have been increasing alarmingly. Ring cameras, for example, were breached, allowing attackers to use the hacked cameras to threaten their

[316] https://blog.lumen.com/the-resilient-satori-botnet/
[317]https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/brickerbot-malware-permanently-bricks-iot-devices
[318] https://pierrekim.github.io/blog/2017-03-08-camera-goahead-0day.html
[319]https://www.trendmicro.com/vinfo/pl/security/news/cybercrime-and-digital-threats/millions-of-networks-compromised-by-new-reaper-botnet

victims and use racial slurs.[320] Attackers are also becoming increasingly creative in their attack methods. The database of one casino was accessed by attackers exploiting the thermostat of a fish tank in the lobby of the casino.[321]

- **CPS** - All aforementioned attacks, although devastating and impacting, typically involved only the stealing of some valuable information (database, credentials, etc.). With the advent of CPS, combined with the ever increasing creativity of attackers, however, even the physical wellbeing of victims is now being threatened. Attackers knocked out the heating systems of two apartment buildings in Lappeenranta, Finland, for example, leaving the residents exposed to the biting November cold.[322] Healthcare IoT devices (pacemakers and defibrillators) have also been identified by the US FDA[323] to be in imminent danger of being controlled by attackers.

All these attacks that were earlier typically carried out on individuals or institutions have over time evolved into state-level attacks. Critical infrastructure and military targets have become targets of cyberattacks. Drones, for example, have been demonstrated to be vulnerable to cyberattacks.[324] In a YouTube video,[325] the authors show how drone manufacturing can be exploited by a phishing attack, resulting in a defective rotor blade on the drone, causing the drone to crash at a point in time of the attacker's choosing. Numerous other attacks on critical infrastructure, such as those on Iran's nuclear power plant (Stuxnet[326]), the Ukrainian power grid,[327] and Belgium's Internet services,[328] all prove that critical infrastructure is no longer beyond the reach of attackers, and cyberspace is the new battlefield in modern times.

5.5 Use of websites and hosting services

In the modern era, as the Internet has become an integral part of our lives, much business is conducted online. The mechanism for conducting such business is websites. Be it a small-sized (less than 10 employees) company, or a Fortune 500 company, establishing and growing an online presence via websites is essential. As websites evolved from being mere static pages to those serving personalised dynamic content, so was there an increase in the number of components required to support such websites (e.g. databases). As the amount of private information increased, so did the cybercriminals' attempts to attack such websites.

Irrespective of how complex a website is, however, from the point of view of an attacker, a website possesses the following features:[329]

- a server (i.e. resources) that can be misused to run malware

[320] https://www.theguardian.com/technology/2020/dec/23/amazon-ring-camera-hack-lawsuit-threats
[321] https://www.washingtonpost.com/news/innovations/wp/2017/07/21/how-a-fish-tank-helped-hack-a-casino/
[322] http://metropolitan.fi/entry/ddos-attack-halts-heating-in-finland-amidst-winter
[323]https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities-0
[324] https://www.kaspersky.com/resource-center/threats/can-drones-be-hacked
[325] https://www.youtube.com/watch?v=zUnSpT6jSys
[326] https://www.mcafee.com/enterprise/en-us/security-awareness/ransomware/what-is-stuxnet.html
[327] https://jsis.washington.edu/news/cyberattack-critical-infrastructure-russia-ukrainian-power-grid-attacks/
[328] https://www.euronews.com/2021/05/05/belgium-s-parliament-and-universities-hit-by-cyber-attack
[329] https://xneelo.co.za/help-centre/website/why-would-my-site-be-hacked/

- a possible clean reputation up for grabs
- interesting user data (possibly)
- user traffic
- other features important to its owner

All these are opportunities for the attacker to creatively exploit and make money. In the end, the goal is almost always to make money.

We now describe with examples how attackers can compromise a website and how a compromised website can further be misused for malicious gains:

- Domain hijacking and traffic redirect. Attackers can target hosting services that also provide domain registrations. Compromising such a hosting service allows the attacker to alter the DNS records of benign domains, thereby redirecting incoming traffic away from websites hosted on those domains to malicious machines serving exploit kits. An example of such an attack was encountered by the French domain registrar Gandi,[330] where 751 customer domains were hijacked to redirect traffic to an exploit kit.
- Another approach taken by, for example, the Neutrino exploit kit, is to use a Domain Generation Algorithm to generate new and cheap domains[331]. These malicious domains are frequently registered on freely available country code top level domains (ccTLD) and are set up to host the Neutrino exploit kit. Attackers then proceed to compromise a web server, and trigger a URL redirect to the malicious domain whenever a user visits the compromised web server. The URL redirect downloads the malware (Neutrino exploit kit or other malware including ransomware) that can exploit the user based on a range of applicable vulnerabilities.
- Malvertising is an attack in which the attackers inject malicious code into legitimate digital advertisements shown on websites. Malvertising takes undue advantage of the complex network of digital advertising. Typically, the attack begins by the compromise of a third-party server, allowing the attackers to inject malicious code within a display ad. As a result, whenever a user visits the website, the infected advertisement is displayed and the malicious code is executed on the user's browser. Such malicious code typically redirects users to another malicious website, where a malware or an exploit kit may be installed on the user's machine. Malvertising also targets high profile brands to take advantage of the high web traffic already generated by such brands' websites. In the past, attackers have resorted to malvertising by targeting brands such as Spotify,[332] the New York Times and the BBC.[333]
- Cryptocurrency mining. This is an attack where the attacker intends to use the underlying hardware on which a website is hosted. Attackers compromise the hosted website, thereby making it possible to access the resources. Attackers can then (mis)use the available resources as they deem fit. Cryptocurrency mining is a typical avenue

[330] https://www.bleepingcomputer.com/news/security/751-domains-hijacked-to-redirect-traffic-to-exploit-kits/
[331] https://blog.angelalonso.es/2016/03/hunting-exploit-kits-in-enterprise.html
[332] https://www.theguardian.com/technology/2016/oct/06/spotify-hit-by-malvertising-in-app
[333]https://www.theguardian.com/technology/2016/mar/16/major-sites-new-york-times-bbc-ransomware-malvertising

taken by attackers to use stolen resources for generating money. Such cryptomining attacks have been conducted previously on WordPress websites.[334] In the example attack, WordPress sites were compromised by a brute-force dictionary attack on the login credentials. Once compromised, the resources were used to carry out computations for the Monero crypto currency. The compromised website then conducted additional brute-force attacks to recruit more victims to its botnet. It should be noted that the compromised website was hosted on a Virtual Private Server (VPS), which is a type of shared hosting. Therefore, a website compromised on such hosts can guarantee the attacker more resources along with a likelihood of attacking more websites on the same shared host.

- Leveraging your reputation. This is an important criterion for attackers. If a website is marked as clean, then an attacker can take advantage of it. Whether it involves grabbing traffic or exploiting a website's good name, an attacker will be interested in a website if it has a clean reputation. If the website of interest has a popular rating, then it is even better. The goal of the attackers in such cases is to host their own malicious content. In other cases, compromising websites with clean reputation allows attackers to redirect all the unsuspecting traffic from the original websites to a different malicious website.

5.6 Social engineering, use of 'human' vulnerabilities

We have also reviewed ways in which human factors influence technical and business strategies and criminals' choices. The human factor is often highlighted as the weakest link in cybersecurity. According to the UK Information Commissioner's Office, in 2019 the propoertion of UK data breaches caused by human error reached 90%.[335] Attackers are transitioning away from technical-based attacks to attacks designed to coerce or influence the accidental insider into making exploitable errors.[336]

Social engineering is defined by the European Union Agency for Cybersecurity (ENISA) as the techniques aimed at talking a target into revealing specific information or performing a specific action for illegitimate reasons.[337] There are many different types of social engineering techniques. While some techniques use a "spray and pray" approach and rely on a small percentage of targets falling victim to the attack, other techniques aim to target a single high-value individual. Examples of social engineering techniques include:

- **Phishing** – an attempt to trick users into doing "the wrong thing" through email, social media, SMS (smishing) or over the phone (vishing)
- **Spear phishing** – a more sophisticated version of phishing attack that targets specific organisations or individuals

[334] https://www.wordfence.com/blog/2017/12/massive-cryptomining-campaign-wordpress/
[335] CybSafe, "Human error to blame for 9 in 10 UK cyber data breaches in 2019", 2020. https://www.cybsafe.com/press-releases/human-error-to-blame-for-9-in-10-uk-cyber-data-breaches-in-2019/
[336] D. Norman et al, Human-Centred Security: Addressing psychological vulnerabilities, Information Security Forum, 2019, pg.1
[337] ENISA, "What is "Social Engineering"?" https://www.enisa.europa.eu/topics/csirts-in-europe/glossary/what-is-social-engineering

- **Whaling** – a type of phishing targeting a single high-value individual (typically executives)
- **Baiting** – luring a victim into performing a specific task by providing easy access to something the victim wants
- **Quid pro quo** – requesting confidential information in exchange for compensation
- **Tailgating** – following an authorised person into a restricted area of the system

The various social engineering techniques look to exploit the poor judgement and errors resulting from heuristics and cognitive biases in human decision-making. Examples of heuristics and cognitive biases include:

- **Affect heuristic** – making quick decisions based on an emotional response
- **Anchoring** – relying on the first or most profound piece of information
- **Availability heuristic** – making judgements about the likelihood of an event based on how easily an example comes to mind
- **Bounded rationality** – making "good enough" judgements based on the time available to make a decision
- **Choice overload** – struggling to make decisions when faced with too many options
- **Decision fatigue** – repetitive decision-making tasks strain mental resources
- **Ego depletion** – humans have a limited supply of willpower that decreases with use
- **Herd behaviour** – the tendency for humans to follow the actions of a larger group
- **Licensing effect** – indulging after doing something positive first
- **Optimism bias** – humans believe they are at less risk of experiencing a negative event compared to others
- **Over-justification effect** – the loss of motivation or interest after receiving excessive external rewards
- **Polarisation** – seeing things as either/or with no grey area can lead to individuals thinking in extremes

There are number of notable case studies where cybercriminals have used social engineering techniques for significant financial gain. One example was between 2013 and 2015 where an individual posed as a manufacturer to two of the Big Tech giants, Facebook and Google, and sent spear phishing emails to specific employees invoicing them for goods and services. This resulted in over $100 million being deposited into fraudulent bank accounts.[338] Another example was in 2019, when the CEO of a UK energy provider transferred $243,000 to a scammer who posed as a supplier over the phone. The cybercriminal used AI-based software to mimic a German voice and gain credibility.[339]

[338] BBC, "Google and Facebook duped in huge 'scam'", 2017. https://www.bbc.co.uk/news/technology-39744007
[339] The Wall Street Journal, "Fraudsters used AI to mimic CEO's voice in unusual cybercrime case", 2019. https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402

5.6.1 Influence on the choices of cybercriminals

The nature of social engineering techniques is influenced by the cybercriminal and their choice of potential victim. Depending on the outcome an attacker wishes to achieve and the characteristics of the person they are trying to target, he or she may use one or more of the six types of social power to tailor their chosen technique. The six types of social power are:

1. **Reward power** – the promise of a reward for completing a task
2. **Coercive power** – leveraging fear and punishment to manipulate human behaviour
3. **Referent power** – manipulating individuals to following their idols blindly
4. **Informational power** – using privileged information to increase credibility
5. **Legitimate** – using positions of power to order the completion of tasks
6. **Expert** – impersonating an individual using in-depth information, knowledge or expertise

Another factor influencing the choice of cybercriminals in the type of social engineering they employ is the technical skill and level of resource they possess. While more personal and tailored social engineering techniques may require more skill and resource, typically, social engineering enables attackers who lack the technical skills, motivation to use them or the resources to purchase or hire them.[340]

5.6.2 Influence on technical and business strategies

The exploitation of human vulnerabilities by cybercriminals through social engineering has resulted in the need for organisations to address poor security behaviours. Measures to achieve a reduction in cyber risk from human factors can be both technical and strategic in nature. In terms of technical measures, secure-by-design systems, applications, processes and the physical environment, as well as identity and access management (IAM) policies and tools, can be employed. In terms of strategic measures, security awareness programmes are commonly employed by organisations.

Although security awareness programmes or campaigns are among the most popular measures employed by organisations, a number of limitations have been identified. These programmes can often be unengaging, not diverse (e.g. too much focus on phishing), a one-off activity and under-resourced.[341] In some cases, security awareness programmes are only conducted to the level of meeting regulatory requirements, which can lead to some employees perceiving them as "tick box" activities. Security awareness campaigns in isolation can often not result in sustained behaviour change or a reduction in the number of security incidents.[342] A multi-layered approach that combines both the technical and business strategies to protect against socially engineered human vulnerabilities will be most effective.

[340] Europol, "Social Engineering", https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/cybercrime/social-engineering

[341] Forbes, "Seven Reasons Why Your Company's Security Training Isn't Working", 2021. https://www.forbes.com/sites/forbestechcouncil/2021/06/09/seven-reasons-why-your-companys-security-training-isnt-working/

[342] D. Norman et al, Human-Centred Security: Positively influencing security behaviour, Information Security Forum, 2020, pg.1

5.7 Supply chain attacks

In recent years, supply chain attacks have become more and more common. The attacks targeted different types of utility software, such as text editors, video players, file managers and many others. Other attacks abused open-source code repositories that can also affect organisations. The type of software and services that have been targeted in the observed targeted attacks can be summarised in the table below (F-SECURE, 2021):

Type of software	Targeted (%)
Utility	32%
Application	24%
Others	22%
Code repository	12%
Managed service provider	5%
Software hosting	5%

Here we describe the most notable supply chain attacks documented since 2011 (F-Secure, 2021).

2011

- ESTsoft ALZip software (Threat: Backdoor.Agent.Hza)
    - Attackers uploaded a backdoor to a server used for releasing updates of ALZip, a compression application from a South Korean software company ESTsoft. The upgrades containing the backdoor compromised 62 PCs at SK Communications, allowing attackers to steal user IDs, passwords, and other sensitive information and access databases for the telecom's Cyworld social networking website and the Nate web portal. It was believed to be South Korea's biggest theft information incident.[343]
- Computer game publisher (Threat: Winnti)
    - A computer game publisher was found spreading a trojan through its official update server. Investigations revealed that it was related to a hacking group named Wintti, a group known to specialise in cyberattacks against the online

[343] https://www.theregister.com/2011/08/12/estsoft_korean_megahack/

video game industry. Although the group's main objective was believed to be stealing source codes for online game projects and digital certificates of legitimate software vendors, the cyberattack placed a piece of malware on a game's official update server, causing it to be delivered to its players as part of a regular update.[344]

2013

- Simdisk (Threat: Castov)
  - A trojan downloader known as Castov was discovered delivered through a trojanised version of a legitimate software, Simdisk. It was distributed through a compromised website. When a user downloaded and executed it, it dropped the legitimate Simdisk application and the malicious downloader, which downloads additional components that perform DNS requests to overload the Gcc.go.kr DNS server, effectively performing a DDoS attack.[345]

2014

- GOM Player (Threat: Miancha)
  - A trojanised update for GOM Player, a free media player, delivered Miancha Backdoor. The trojanised update was reported to possibly affect a PC associated with "Monju" (the Fast Breeder Reactor of the Japan Atomic Energy Agency). The media player was said to be favoured by many Japanese people and its users were said to be more than 6 million in Japan.[346]
- ICS/SCADA manufacturer sites (Threat: Havex)
  - Industrial Control Systems (ICS)/Supervisory Control and Data Acquisition (SCADA) manufacturer websites were found to have trojanised software installers made available for download, as part of an industrial espionage attack. The trojanised software included Havex, a general purpose Remote Access Trojan (RAT), and was used to gather details on ICS/SCADA hardware connected to infected devices.[347]

2015

- League of Legends & Path of Exile (Threat: PlugX)
  - Official game files for League of Legends (LoL) & Path of Exile (PoE) were trojanised by cybercriminals by bundling them with the PlugX Remote Access Trojan (RAT). The games were distributed in certain Asian countries by Singapore-based Garena.[348]
- EvLog (Threat: Kingslayer)
  - An attacker group known as Kingslayer obtained the private signing key of Altair Technologies, and used it in order to sign a trojanised version of their EvLog product. The trojanised version of EvLog was made available to its users as part of a software "upgrade". Evlog is software used by system administrators

[344] https://securelist.com/winnti-more-than-just-a-game/37029/
[345]https://community.broadcom.com/symantecenterprise/communities/community-home/librarydocuments/viewdocument?DocumentKey=edd5c93e-7160-4bf2-a15c-f1c024feb0d7&CommunityKey=1ecf5f55-9545-44d6-b0f4-4e4a7f5f5e68&tab=librarydocuments
[346] https://securelist.com/abused-update-of-gom-player-poses-a-threat/58240/
[347] https://archive.f-secure.com/weblog/archives/00002718.html
[348] https://www.securityweek.com/plugx-rat-distributed-official-game-installers

to analyse event logs. Numerous organisations using the product were affected by this attack, including telecommunication providers, military organisations, government, financial, education institutions and other solution providers.[349]

- Xcode (Threat: XcodeGhost)
    - Attackers successfully uploaded a Trojanised version of Xcode, a tool used by developers to build iOS apps. This incident led to the first major attack on Apple's App Store, infecting hundreds of legitimate iOS apps with the embedded malware XcodeGhost.[350]

2016

- Transmission (Threats: OSX KeRanger & OSX Keydnap)
    - Recompiled malicious versions of Transmission BitTorrent client installers for OSX were found distributed on its official website. In March 2016, the malicious installers contained ransomware named KeRanger.[351] Later in August 2016, new malicious versions were found distributing Keydnap, a backdoor that also steals the content of OSX's keychain.[352]
- MSP (Threat: CloudHopper)
    - APT10, a hacking group also known as Stone Panda, POTASSIUM, MenuPass and Red Apollo, conducted a widespread cyber espionage campaign by compromising Managed IT Service Providers (MSPs) as an attack vector to infiltrate the networks of its clients. The MSP clients that were affected consisted of offices related to engineering, industrial manufacturing, retail, energy, pharmaceuticals, telecommunications, and government agencies.[353]
- Linux Mint (Threat: backdoor)
    - The website of Linux Mint was compromised and was found to be serving a malicious version of one of the 64-bit Linux distribution images (ISO) that contained a backdoor.[354]
- FossHub (Threat: MBR writer)
    - FossHub, a free software site, was compromised by hackers and two popular programs it serves were replaced with malware. One of these was Audacity, a popular audio editing and recording program. FossHub was able to detect and remove the malicious file before anyone downloaded it. The other targeted program was Classic Shell, a Start menu program replacement, which was reported to have had 300 downloads before FossHub shut it down. Once downloaded, the malicious file nuked the master boot records (MBR) of the victim's machine.[355]
- Ask Partner Network (Threat: banking trojans)

[349] https://comsecglobal.com/kingslayer-a-supply-chain-attack/
[350] https://www.businessinsider.com/apps-by-attack-on-apple-app-store-2015-9?r=US&IR=T
[351] https://unit42.paloaltonetworks.com/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/
[352] https://www.welivesecurity.com/2016/08/30/osxkeydnap-spreads-via-signed-transmission-application/
[353] https://cyberlaw.ccdcoe.org/wiki/Operation_Cloudhopper_(2017)
[354] https://www.zdnet.com/article/hacker-hundreds-were-tricked-into-installing-linux-mint-backdoor/
[355]https://www.pcworld.com/article/3104180/pc-nuking-malware-sneakily-replaces-popular-free-software-on-fosshub.html

- Ask.com Toolbar's update feature was compromised, causing the toolbar update to install a dropper into the users' browsers. The dropper, once installed, brought secondary payloads that included banking trojans, and other online-fraud code.[356]

2017

- M.E.doc (Threat: NotPetya)
  - Threat actors manipulated the update server for M.E.Doc software by using stolen credentials, and delivered destructive malware disguised as ransomware as part of the software's update system. M.E.Doc is an accounting software package created by the Ukrainian company, Intellect Service. It is widely used in Ukraine, and used to interact with Ukrainian tax systems. The malware functionality included file encryption and overwriting of the victim's boot sector or wiping sectors of the physical drive. The attack caused extensive damage to organisations in Ukraine, and across the world.[357]
- UltraEdit (Threat: WilySupply)
  - UltraEdit's software update system was compromised, causing its software update to deliver a malicious binary. The operation was dubbed as WilySupply, and involved Powershell scripts bundled with the Meterpreter reverse shell launched by the malicious binary, giving a remote attacker silent control.[358]
- HandBrake (Threat: OSX Proton)
  - The Handbrake app was replaced by attackers with a malicious app on its official website. Handbrake is free software used for converting videos from a variety of formats to a supported codec. Its handlers reported that one of its mirror-download servers was compromised so that it served the malicious app, installing a malware named Proton, a professionally developed backdoor sold on the Dark Web.[359]
- Leagoo (Threat: Android Triada)
  - An Android trojan named Triada was found pre-installed on low-cost Android devices. The malware was embedded in a modified system library that can penetrate the processes of all running app without requiring root privileges. The affected devices include Leagoo M5 Plus, Leagoo M8, Nomu S10, and Nomu S20.[360]
- NetSarang (Threat: ShadowPad)
  - Modified versions of server management software distributed by NetSarang Computer, Inc., from its official website were found to include an encrypted payload. The backdoor, known as ShadowPad, was embedded into one of the code libraries used by the software. Companies that rely on NetSarang's software were affected; they included the banking and financial industry,

[356]https://www.csoonline.com/article/3143131/attacks-to-make-ask-com-toolbar-a-conduit-for-malware-are-nipped-in-the-bud.html
[357] https://blog.talosintelligence.com/2017/07/the-medoc-connection.html
[358]https://www.microsoft.com/security/blog/2017/05/04/windows-defender-atp-thwarts-operation-wilysupply-software-supply-chain-cyberattack/?source=mmpc
[359]https://blog.malwarebytes.com/threat-analysis/mac-threat-analysis/2017/05/handbrake-hacked-to-drop-new-variant-of-proton-malware/
[360] https://www.securityweek.com/triada-trojan-preinstalled-low-cost-android-devices

software and media, energy and utilities, computers and electronics, insurance, industrial and construction, manufacturing, pharmaceuticals, retail, telecommunications, transportation and logistics and other industries.[361]

- CCleaner (Threat: Floxif)
    - Versions of CCleaner were modified by hackers and were bundled with a trojan named Floxif. The malware's functionality included sending stolen information from a victim's machine to a remote attacker, including the computer name, installed software, running processes, and MAC addresses.[362]
- PyPI repository (Threat: typosquatting)
    - Malicious software libraries were uploaded by attackers in the official Python package repository. The malicious packages had filenames nearly identical to or easily confused with the legitimate ones. There was evidence that the malicious packages were downloaded multiple times between June 2017 and September 2017.[363]
- Elmedia Player (Threat: OSX Proton)
    - Eltima, makers of Elmedia Player software, were found to be distributing a trojanised version of their application with Proton malware on their official website.[364]
- IBM Storwize (Threat: Reconyc)
    - A malicious file distributed on USB flash drives was identified by IBM. The malicious file was copied to the user's machine when the initialisation tool was launched on the USB flash drive for IBM Storwize V3500, V3700 and V5000 Gen 1 systems. However, it was not executed during initialisation.[365]
- WordPress repository (Threat: backdoors)
    - A WordPress plugin, Captcha, was compromised by attackers and delivered a trojanised version that downloads and installs a hidden backdoor. The backdoor was included in the WordPress Plugin, with more than 300,000 installations.[366]

2018

- MediaGet (Threat: Dofoil)
    - A trojanised version of MediaGet, a BitTorrent client, was distributed through the software's update system. The attackers compromised the update server and replaced the software with a nearly identical but malicious binary that dropped Dofoil malware (also known as Smoke Loader). This eventually led to installation of a Coinminer, attempting to use the victim's computer resources to mine cryptocurrencies for the attackers. There were 400,000 infections reported, affecting users in Russia, Turky and Ukraine.[367]
- MEGA Chrome extension (Threat: cryptocurrency stealer)

[361] https://securelist.com/shadowpad-in-corporate-networks/81432/
[362] https://www.bleepingcomputer.com/virus-removal/remove-floxif-ccleaner-trojan
[363] https://www.nbu.gov.sk/skcsirt-sa-20170909-pypi/
[364] https://www.welivesecurity.com/2017/10/20/osx-proton-supply-chain-attack-elmedia/
[365] https://www.ibm.com/support/pages/node/697231
[366] https://www.bleepingcomputer.com/news/security/backdoor-found-in-wordpress-plugin-with-more-than-300-000-installations/
[367]https://www.microsoft.com/security/blog/2018/03/13/poisoned-peer-to-peer-app-kicked-off-dofoil-coin-miner-outbreak/

    - The Google Chrome extension, MEGA (a popular file upload and sharing service), was compromised by hackers. The compromised version of the extension was actively monitoring user information stored in the browser.[368]
- Magecart attacks
    - A threat group known as Magecart, focusing on stealing payment information entered into online payment forms, compromised a number of third-party components shared by many of the most frequented e-commerce sites in the world as a massive digital credit card-skimming campaign. Third-party providers such as Inbenta (Chatbot provider), SociaPlus, PushAssist, and Annex Cloud were reported to be compromised suppliers for e-commerce sites, and were used to serve malicious scripts with skimming functionality. One of the biggest victims was TicketMaster, a ticket sales and distribution company, which was using components from compromised suppliers.[369]
- PDF Editor application (Threat: cryptominer)
    - Attackers tried to create a clone of PDFEscape, a PDF Editor application, by creating a similar infrastructure on a server under their control. The attackers copied all the installer packages and modified one of the installers to deliver a crypto miner to the victim's machines.[370]
- Remote support solutions provider (Threat: 9002 RAT)
    - A remote support solutions provider was compromised by attackers to deliver a remote access trojan named 9002 RAT through its software update system. The attackers stole the company's certificate to sign malicious files and configured the update server to deliver them to IP addresses belonging to targeted organisations.[371]
- Webmin (Threat: backdoor)
    - A version of Webmin, a systems-management user interface tool that is widely used in Unix-based environments, was released with a backdoor that could allow a knowledgeable attacker to execute its commands as root. The Webmin build system was compromised in April 2018, and the attacker rolled back the timestamp on the build back to prevent users noticing the added malicious code in the codebase. It was detected in 2019, which means the malicious version was served and downloaded by users for more than a year. [372]
- Event-stream npm package (Threat: cryptocurrency stealer)
    - A trojanised version of the Node.js library listed in NPM's warehouse of repositories was found to contain crypto-coin stealer malware. This library was downloaded roughly two million times a week by application programmers.[373]
- Docker Hub (Threat: cryptominer)

[368] https://www.ccn.com/hacked-mega-chrome-extension-was-used-to-steal-cryptocurrency/
[369] https://www.riskiq.com/blog/external-threat-management/magecart-ticketmaster-breach/
[370] https://blog.comodo.com/pc-security/cryptomining-executed-through-legitimate-software/
[371]https://www.trendmicro.com/en_fi/research/18/h/supply-chain-attack-operation-red-signature-targets-south-korean-organizations.html
[372]https://www.zdnet.com/article/backdoor-found-in-webmin-a-popular-web-based-utility-for-managing-unix-servers/
[373] https://www.theregister.com/2018/11/26/npm_repo_bitcoin_stealer/

- Malicious images in Docker Hub were used to spread Monero-mining malware to unsuspecting cloud developers. The malicious images were reported to have a total of 20 million downloads over a span of at least two years.[374]

2019

- Asus live update (Threat: ShadowHammer)
  - Asus Live Update Utility, which comes pre-installed on most ASUS computers as a trusted automatic software update tool for certain components, drivers, and applications, was compromised by attackers known as ShadowHammer, and was believed to have pushed malware to thousands of computers.[375]
- DoorDash (Threat: unauthorised access to user data)
  - An unauthorised third-party access on their user data was detected by DoorDash, a food-delivery company, affecting 4.9 million consumers, merchants, and delivery people on its platform.[376]

2020

- Github (Threat: Octopus Scanner)
  - A set of GitHub-hosted repositories were detected to serve malware named as Octopus Scanner. This malware targeted the Apache NetBeans Java integrated development environment (IDE) used to develop the Java-based desktop, mobile and web applications, as well as HTML5 applications with HTML, JavaScript and CSS.[377]
- RubyGems (Threat: cryptocurrency stealers)
  - Threat actors uploaded typosquatted malicious libraries to RubyGems, a package manager that contains open-source components (known as "gems") for the open-source Ruby programming language code base, which can be used as basic application building blocks by software developers. There were 760 malicious libraries identified in the said repository, including a cryptocurrency stealer.[378]
- Able Desktop (Threat: backdoors)
  - Able Desktop, a type of chat software known to be part of a business management suite popular in Mongolia and used by 430 government agencies in that country, was found to deliver several backdoors or remote access trojans such as HyperBro, PlugX (also known as Korplug RAT), and Tmanger RAT.[379]
- VGCA (Threat: PhantomNet)
  - Modified versions of two of the software installers available for download on the website of the Vietnam Government Certification Authority (VGCA) included a backdoor in order to compromise users of the legitimate application. The cybercrime operation was dubbed SignSight, and involved a malware known as PhantomNet or Smanager. The malware's functionality included

[374]https://www.bleepingcomputer.com/news/security/docker-hub-images-downloaded-20m-times-come-with-cryptominers/
[375] https://securelist.com/operation-shadowhammer/89992/
[376] https://blog.doordash.com/important-security-notice-about-your-doordash-account-ddd90ddf5996
[377] https://securitylab.github.com/research/octopus-scanner-malware-open-source-supply-chain/
[378] https://threatpost.com/bitcoin-stealers-700-ruby-developer-libraries/154937/
[379] https://www.welivesecurity.com/2020/12/10/luckymouse-ta428-compromise-able-desktop/

collecting the victim's information and the installation/removal/update of malicious plugins.[380]

- Websites that support WIZVERA VeraPort (Threat: Lazarus)
    - Lazarus, a cybercriminal group known for the Sony Pictures Entertainment hack, targeted a security software called Wizvera VeraPort. This software was used by South Korean government websites, where visitors are required to use a VeraPort browser plug-in for identity verification. The attack started with Lazarus operators achieving a foothold on the Wizvera software server. This allowed the planting of malicious binaries, which appear to be legitimate, but use the stolen digital certificates on a compromised website and are pushed automatically to unsuspecting site visitors.[381]
- Noxplayer (Threat: backdoors)
    - Attackers compromised the software update system of NoxPlayer, a popular Android emulator for PCs and Macs. NoxPlayer queries the update server via BigNox HTTP API to check for updates and retrieves update-related information. Researchers believed that certain sections of the BigNox infrastructure were compromised to deliver malicious updates involving a backdoor and remote access trojan.[382]
- Solarwinds (Threats: Sunspot, Sunburst, Teardrop)
    - Attackers targeted the SolarWinds Orion IT management product by deploying a Sunspot,[383] which injects malicious code into the SolarWinds platform during its software build process. The attack involved monitoring the processes involved in the compilation of the Orion product and replacing one of the source files to include a backdoor dubbed as Sunburst.[384] It was later deployed as part of the software's update packages. The Sunburst backdoor was then used to deploy different payloads, which researchers so far have named Teardrop and Raindrop.[385] SolarWinds is a leading provider of network performance monitoring tools used by many organisations across the globe, and the victims of this attack included government, consulting, technology, telecom and extractive entities in North America, Europe, Asia and the Middle East.

2021

- Open-source repositories (Threat: dependency confusion)

Qentinel, a cloud-based test automation solution provider, became a target of a dependency confusion attack—a supply chain attack technique in which an attacker uploads malicious packages to public repositories to be pulled by developers for installing dependencies for their projects using package installer tools such as Python's pip (PyPI - Python Package Index). In the case of Qentinel, three main libraries used by their testing platform had all been created by an unknown account in the package repository PyPI. Because of the way pip is constructed, it

[380]https://www.eset.com/us/about/newsroom/press-releases/eset-discovers-operation-signsight-supply-chain-attack-against-a-certification-authority-in-southea-1/
[381] https://threatpost.com/hacked-software-south-korea-supply-chain-attack/161257/
[382] https://www.welivesecurity.com/2021/02/01/operation-nightscout-supply-chain-attack-online-gaming-asia/
[383] https://www.crowdstrike.com/blog/sunspot-malware-technical-analysis/
[384]https://www.fireeye.com/blog/threat-research/2020/12/evasive-attacker-leverages-solarwinds-supply-chain-compromises-with-sunburst-backdoor.html
[385] https://www.zdnet.com/article/fourth-malware-strain-discovered-in-solarwinds-incident/

fetched the malicious libraries from PyPI instead of the actual libraries from their private repositories.[386]

5.8 Attacks on cloud platforms

As discussed in section 3.12, cloud technologies offer a large range of tools that cybercriminals may use to facilitate their attacks. Cloud adoption has not only provided attackers with new facilities to utilise, but it has also changed the threat landscape for businesses moving to cloud. These changes have come in the form of attack surface complexity, changes in responsibilities and division of administration. Many organisations are using cloud services provided by multiple different providers, each with their own roles and permissions. This complexity in volume means that enforcing the "least privilege" principle is difficult, which in turn leaves identity and access management (IAM) susceptible to misconfigurations. Overly permissive access is common[387] and, as seen in the Solarwinds attacks,[388] it can be leveraged for further exploitation.

Cybercriminals have much the same objectives in the cloud as they have when attacking more traditional on-premise environments, with the end goal being monetisation. Some of the most common types of attacks are deploying ransomware, data theft, cryptojacking and DNS hijacking. It is common that the initial attacker who gains access to the environment is not the one who deploys the final payload. Access keys and credentials are routinely being sold by initial access brokers (IAB) on Dark Web forums.

5.8.1 Malware delivery

Cloud applications have become the most common source of malware. Reports in 2020[389] showed that up to 61% of malware, trojans and payloads were being hosted by popular cloud applications. By using cloud applications as a delivery channel, the attackers aim to circumvent the blocklists and abuse the implicit trust users have in service providers. Using cloud applications as hosting services, the cybercriminals can easily host their content on a reputable domain, with genuine SSL certificates, thus evading easy detection. This also gives them the benefits of agile deployment and limited traceability, as mentioned in section 3.12. This technique includes, for example, hosting second-stage payloads on services like Github, or malicious docker images on Docker Hub.

5.8.2 Cloud as a phishing platform

Wide adoption of cloud services has also brought new dimensions to phishing tactics. Cloud service credentials have become one of the major targets of the traditional credential phishing attacks. The attackers deploy a multitude of different tricks, from appearing as a cloud service provider needing an action from the customer, to sharing a document describing a pay raise to get the user to open a link to a cloud-hosted file. Commonly, these links take the user to a fake

[386] https://info.qentinel.com/blog/dependency-confusion-attack
[387] https://unit42.paloaltonetworks.com/iam-misconfigurations
[388] https://www.atlanticcouncil.org/in-depth-research-reports/report/broken-trust-lessons-from-sunburst/
[389] https://resources.netskope.com/cloud-security-infographics/cloud-and-threat-report-february-2020

login page, asking the user to log in to view the file. When the login credentials are entered, they are exfiltrated to the attackers via email or using services like Telegram or Google Forms.[390]

Cybercriminals have also found ways to turn the service providers' own services against its customers. For example, Google's applications, including Calendar, have been used to evade the Gmail filters, creating fake meeting invitations with links to phishing sites.[391]

Another commonly used phishing technique that is especially targeting organisations using cloud services is consent phishing. These attacks abuse cloud service providers' use of the OAuth 2.0 authorisation mechanism, a protocol that is used to allow third-party applications to perform actions on the user's behalf and to access their data. In these attacks the victim is lured to grant permissions to a malicious cloud application, often posing as a credible publisher, imitating other applications or presenting as an utility application. In some cases the consent phishing applications have only requested read-only access to the victim's email, to then later leverage the gathered information for business email compromise (ccTLD attacks. Consent phishing attacks are usually executed via distributing phishing emails with installer URLs.

5.8.3 Account compromise

Cloud services are identity centric and account compromise is a key way of entry. Attackers use various means to obtain valid credentials or access keys to the cloud. Credential exposure is a common way of compromising a cloud account. Cybercriminals are actively scanning online data, for example in Github or Bitbucket repositories, for leaked credentials or access keys. Another common attack vector is credential stuffing. Credential stuffing is not a new technique in the cybersecurity world, but it is still a valid one and also applies to the cloud. It is still a commonly used and effective technique. In a credential stuffing attack, the attacker may use a list of usernames and passwords either generated or obtained from a breached database. The attacker may use a network of bots to send login attempts to a target, using rate limiting to evade login protections.

5.8.4 Misconfiguration abuse

On-demand scalable data storage has seen a considerable rise in adoption and that has also been seen in the quantity of data breaches. As highlighted in the resource hijacking section, misconfigurations of cloud instances have unfortunately been common, and that has resulted in a number of cloud storage buckets exposed to the public. The list of breached Amazon S3 buckets is extensive and includes many high-profile companies. Although common, data stealing has not been the only way unsecured S3 buckets have been abused by cybercriminals. The Magecart threat actor, conducting credit card skimming attacks by injecting malicious javascript code into payment pages, was also reported[392] to have abused unsecured S3 buckets. The attackers executed a widespread attack method of appending malicious credit card skimmer

[390]https://www.bleepingcomputer.com/news/security/google-forms-and-telegram-abused-to-collect-phished-credentials/
[391]https://www.kaspersky.com/blog/spam-through-google-services/27228/
[392] https://www.riskiq.com/blog/labs/magecart-amazon-s3-buckets/

javascript code to all javascript files they found in unsecured S3 buckets, aiming to get their code run on a payment processing site as a means of obtaining victims' credit card details.

5.8.5 Resource hijacking in the cloud

Over the last five years, cryptocurrencies have emerged as a considerable medium of exchange and this development has not gone unnoticed by cybercriminals. Cryptocurrencies have provided cybercriminals with a new, efficient way of transferring money. Since cryptocurrency networks need mining to provide validation of transactions, and miners are essentially exchanging their computational power for rewards, a new avenue of exploitation was born: resource hijacking to perform cryptomining (cryptojacking). Since cryptojacking requires considerable amounts of computing power, from a cybercriminal point of view it pairs perfectly with the almost unlimited on-demand computing resources of cloud service providers. In 2020, cryptojacking was reported to affect globally at least 23% of organisations with a cloud infrastructure.[393] Cybercriminal cryptojacking operations in the cloud have mainly consisted of worm-like malware, which abuses misconfigurations of systems including Docker daemons[394] and Kubernetes clusters.[395] These misconfigurations have left the systems open for unauthenticated users to connect, execute commands and launch the malware. Other types of operations have targeted features or vulnerabilities in specific CSPs' products.

5.9 Attacks on collaboration platforms and tools

Collaboration among teams has always been an integral aspect of businesses. Even in the pre-Internet era in the 90s, collaboration happened via telephone, post, or even telegrams. Computer documents were also created, but would still be stored on individual machines. Such collaboration, even though slow and non-scalable, still existed. This reflected the nature of businesses at that time, which were mostly in the same place and same time zone. With the advent and popularisation of the Internet, however, the fundamental nature of businesses has changed. Businesses commonly started operating as multinational, multicultural entities, functioning across multiple time zones.[396] This necessitated different types of communication among teams, thereby requiring the invention and adoption of new types of collaboration tools and platforms.

As the requirement of instant communication increased, it resulted in the creation of tools such as Skype, and other instant messengers. These were followed in popularity by cloud platforms for creating and sharing documents (e.g. Google and Microsoft cloud platform). Several other specialised tools (for specific tasks) such as Jira, have also been created over the last few years. Because of the extra training time required to acclimatise people to special tools over a period of time, a need for "all in one" tools has grown simultaneously (e.g. Microsoft Teams).

[393]https://www.paloaltonetworks.com/resources/research/unit-42-cloud-threat-report-2h-half-2020-executive-summary
[394] https://unit42.paloaltonetworks.com/docker-honeypot
[395] https://unit42.paloaltonetworks.com/hildegard-malware-teamtnt/
[396]https://www.fh-wedel.de/fileadmin/Mitarbeiter/Records/Trillmich_2019_-_The_evolution_of_collaboration_tools_to_facilitate_internal_collaboration_.pdf

In 2020, when the COVID-19 pandemic hit the world, the work environment saw an overnight paradigm shift. Most people started working from home, and needed robust collaboration in a virtual environment. Collaboration tools have consequently seen multitudes of changes as well. For example, pre-existing collaboration tools, such as Zoom, were adopted on a much larger scale,[397] whereas other tools such as Microsoft Teams underwent a feature overhaul.

Such large-scale adoption of collaboration of tools has also sparked the interest of attackers. Where the general public sees collaboration opportunities, attackers started seeing exploitation opportunities. As a result, the number of attacks during the pandemic increased accordingly.[398] Peculiar intrusions by strangers during video conference calls became frequent, leading to the coining of the term "zoombombing".

We now describe some attacks that have happened specifically on the following popular collaboration tools and platforms:

- **Zoom** - This video conferencing tool gained immense popularity during the pandemic. Unfortunately, apart from its number of downloads, its list of vulnerabilities also grew. In the initial days of the pandemic (early 2020), there were plenty of attacks on Zoom. The most popular among those was "zoombombing" which allowed unauthorised users to drop in a zoom meeting just by guessing the meeting id. Attackers even sold tools on the Dark Web[399] to automate the process of collecting zoom meeting addresses for the "benefit" of zoombombing the purchaser of the tool. Another attack discovered against Zoom was one that gave attackers the ability to record Zoom sessions and chat messages without the participants' knowledge.[400] Meanwhile, there were three zero-day bugs discovered in the Zoom client, allowing attackers complete remote control over the computer with Zoom installed.[401] Although not an attack seen in the wild, such research efforts demonstrate the popularity that the Zoom software garners among the general public, thereby prompting intense scrutiny.
- **Microsoft Teams** - This "all in one", or at least "multi-purpose tool", has garnered a lot of popularity lately. So much so that the majority of communication and collaboration within business teams has now moved away from emails to Microsoft Teams. Attacks directly using Microsoft Teams as an attack vector are fewer. However, attackers are adept at compromising Microsoft 365 accounts and then using those same credentials to compromise Teams accounts.[402] For example, as reported by Avanan,[403] a partner organisation's Teams account was compromised and the attacker bided his time for one year, listening on Teams chats, before distributing a remote control trojan to Teams contacts.
- There have been plenty of attempts to break into Microsoft Teams, by researchers as well as attackers. In the case of Teams, however, more vulnerabilities have been reported to Microsoft along with proof-of-concept (PoC) exploits, rather than real

[397] https://www.bbc.com/news/business-52884782
[398] https://www.sciencedirect.com/science/article/pii/S0167404821000729
[399]https://blog.cyberproof.com/blog/threat-actors-share-zoom-hacking-methods-on-the-dark-web
[400] https://blog.morphisec.com/zoom-malware-can-record-meetings-attack-simulation-shows-how
[401]https://www.darkreading.com/vulnerabilities---threats/zoom-joins-microsoft-teams-on-list-of-enterprise-tools-hacked-at-pwn2own/d/d-id/1340626
[402] https://www.avanan.com/blog/microsoft-teams-new-attack-form
[403] https://www.avanan.com/blog/microsoft-teams-new-attack-form

attacks in the wild. Also, Microsoft has been swift with regard to fixing these uncovered vulnerabilities. For example, a vulnerability that recently gained a lot of attention was the one discovered by a researcher at Tenable, Inc. The vulnerability was related to the Power Apps tabs feature that, when opening a new tab, only validated the beginning of the input URL. As a result, attackers could create a fake domain to load their own content.[404] Another crucial MS Teams vulnerability was where the Teams executable could double as a Living off the Land binary. The update command could be misused to run malicious code from a publicly-accessible samba server.[405]

- **Slack** - Slack is a cloud-based suite of collaboration tools and services, including instant messaging, which is being increasingly preferred by organisations over standard email. Like Teams, Slack has been in the news for vulnerabilities discovered in its product, such as the remote code execution vulnerability in the "create snippet" feature that displayed incorrect file types, making it possible for a malicious actor to disguise dangerous files as benign.[406] Despite this, however, and also because of swift action in fixing vulnerabilities, Slack has nevertheless earned a good reputation for some time. Sadly though, this is exactly what the attackers are taking advantage of now. In a recent attack, rather than directly attacking Slack, Slack was indirectly misused to be a host for malware. In a novel spam vector, threat actors used a sacrificial account on Slack (until it got reported), to host the BazarLoader malware,[407] and used this URL when sending phishing messages to innocent victims. The attack relied on the fact that users would click on links when they saw the name "Slack" in the URL, because in the era of remote working, this would hardly appear suspicious.
- **Google Meet** - Apart from the previously discussed names of collaboration tools, during the pandemic, there has been an increase in the use of Google Meet as well. Google Meet, a product of Google, like its competitor Zoom, is not immune to attacks either. "Zoombombing" or "meeting bombing", which became well-known because of Zoom, could also happen in Google Meet as well,[408] although this does not to be possible anymore.

5.10 Cyberstalking

Cyberstalking refers to repeated threats or harassment through electronic mail or other computer-based communication that make a reasonable person fear for his/her own safety (Strawhun et al. 2013, Finn 2004). Research suggests that a non-trivial percentage of people have been the victims of cyberstalking. Although the actual numbers vary from study to study, Strauhun et al. (2013) reported that in their study 20.5% of the participants were victims of cyberstalking while Dreßing at al. (2014) reported a prevalence as high as 43.4%. However,

[404]https://medium.com/tenable-techblog/stealing-tokens-emails-files-and-more-in-microsoft-teams-through-malicious-tabs-a7e5ff07b138
[405]https://www.bleepingcomputer.com/news/security/hackers-can-abuse-microsoft-teams-updater-to-install-malware/
[406] https://hackerone.com/reports/833080
[407] https://news.sophos.com/en-us/2021/04/15/bazarloader/
[408] https://aporlebeke.wordpress.com/2020/05/13/google-meet-bombing-yes-its-a-thing-sort-of/

they said that if stringent definition criteria comparable to those of offline stalking are applied (such as duration of more than two weeks and harassment that provoked fear), it is not a mass phenomenon and the percentage of participants who have experienced cyberstalking drops to 6.3%. Duggan (2017) also reports that around 7% of Americans have experienced cyber stalking.

The Internet and social media can play a significant role in cyberstalking along two important dimensions:

- Social media can be the means for connecting the perpetrator and the victim, and
- Social media can be the mechanism to deliver the harassment.

64% OF THE RESPONDERS AMONG 21,000 PARTICIPANTS IN 21 COUNTRIES FEEL THAT SPYWARE-ENABLED CYBERSTALKING IS JUSTIFIED IF THEY FEEL THEIR PARTNER WAS BEING UNFAITHFUL.

Fansher and Randa (2019) report that about 12.65% of the individuals who reported victimisation noted an offender that the victim initially met through a social media application. They also reported that the most common form of victimisation was cyberstalking, although traditional stalking and sexual assaults were also common. Fansher and Randa (2019) suggest that the process of disclosing personal information over social media, under certain circumstances, represents a pathway to victimisation. To make matters worse, they believe that social media may be an entry point to that pathway. Berry and Bainbridge (2017) suggest that people who spend more time on social media have a higher likelihood of being cyberstalked. To make matters worse, they discovered that experienced Internet users have a higher tendency to be cyberstalked (or at least report that they are cyberstalked) compared to less experienced Internet users.

Cyberstalking and its associated harassment can be implemented using a variety of online techniques: email messages, social media interactions, texts, etc. One of the most insidious techniques is the installation of **spyware** which is software that aims to collect information about the victim, invade its personal life, track her/his movements (through GPS in infected smartphones), snoop on messages and phone conversations, monitor web access, and then use this information to harass, blackmail or even terrorise the victim. Although this sounds difficult, several of the spyware-enabled cyberstalking perpetrators are partners of the victims and have physical access to the smartphones and possibly personal knowledge of the passwords. To understand the extent of this cyberstalking, a recent report by Kaspersky suggests that as many as 64% of the responders feel that such a spyware-enabled cyberstalking is justified if they feel their partner was being unfaithful.[409] This percentage rose to 76% for UK residents. This kind of spyware-enabled cyberstalking of partners is so prevalent that the relevant software category has now its own name: **stalkerware**. From a technical point of view, stalkerware is not significantly different from spyware, but it is their intended use that frequently differentiates

409 https://portswigger.net/daily-swig/cyberstalking-study-uk-residents-most-accepting-of-spyware-to-track-partners-movements

the two categories (Parsons et al. 2019). Stalkerware seems to be prevalent among abusers. For example, Citron (2015) reports that "54% of abusers tracked survivors' cell phones with stalking apps" – or stalkerware. Although Google Play Protect systems and antivirus products can identity stalkerware, there are several difficulties in eradicating it from the victim's phone: (i) it is frequently the victim's spouse who installed the application on the phone, and (ii) some of the stalkerware applications are re-purposed apps that, although they appear to have legitimate purposes (e.g,. find your phone if lost), they may be abused for stalking. As a result, companies still develop stalkerware: a list of several of these companies with an analysis of their operation and data protection can be found in Parsons et al. (2019).

5.11 Identity theft - theft of bank cards

One of the first manifestations of cybercrime (for financial purposes) was credit card theft and trading. One of the first such forums were IRC channels, where anyone, including cybercriminals, were gathering to chat and exchange information. However, since the channels were open to anyone (including police officers), and since they provided little history for the participants, they were quickly replaced by websites (such as www.carder.ru) and web forums such as the "Counterfeit Library" forum (Lusthaus 2018b). One of the first successful such forums was CarderPlanet, which was for stolen credit-card trading. Founded by Russian-speaking individuals, CarderPlanet created a leading network of cybercriminals (see Lusthaus, 2018b). In this aspect, CarderPlanet was influential even after it was closed in 2004, as it created the network whose ties remained alive for several years. In the wake of CarderPlanet's shutdown, several forums and marketplaces emerged: Darkmarket, SilkRoad, Hansa market, etc. which cover not only credit cards, but various other products as well.

Stealing credit card numbers goes way back – even before the proliferation of computers. At that time, people used to search trash cans in shopping malls for credit card slips. Today, cybercriminals use a variety of digital approaches to find credit card numbers - without the need to dive into trash. For example, the cybercriminal (i) may intercept data from a compromised point of sale (where the credit card was used), (ii) may add a (hardware) skimmer to an ATM (that reads that credit card data), (iii) may steal data from a compromised website (where the credit card was used), (iv) may play a "man in the middle" attack to intercept the data "on the fly", etc.

Stealing credit card information does not (per se) produce any financial profit. To make money out of this information, cybercriminals need to find a way to "cash out". To make matters worse, they have a limited amount of time to do so, since the legitimate owners of the credit cards may, sooner or later, discover the theft and report the card as stolen. Thus, stolen credit card data are usually sold to someone else in a market in the dark web (or in a specialised forum much like the CarderPlanet back when the dark web did not exist). There are several reasons behind this immediate sale, including geography specialization. For example, criminals from the (ex) Soviet Union were frequently involved in stealing credit cards issued by banks in the United States (Lusthaus, 2018b). If these cybercriminals attempted to use US cards in the (ex) Soviet Union, the US banks would flag the transactions immediately as they would see a US credit card being used in Eastern Europe. On the contrary, if the card was sold to (and used by) someone on the US (if possible in the zipcode of the credit card's legitimate owner), this would probably not raise any significant suspicions – at least not in the beginning. Thus, although the cards were stolen in Eastern Europe, they were immediately sold in North America (or in the

Western Europe) to be used and get as much profit as possible out of them. Stolen cards were used to transfer money to bank accounts that would later be withdrawn (in cash through an ATM) and send back to the cybercriminals via a money transfer service (such as Western Union) (see Soudijn and Zegers, 2012, and Smith, 2015). This withdrawal and money transfer makes it difficult for police to "follow" the money and easily trace the recipients of the money: the cybercriminals. In addition to these money transfers, stolen cards are used to purchase other goods including pre-paid cards, giftcards etc. These, in turn, were used to purchase goods that could be sold via online market places such as eBay.

The main point in this cybercrime chain was to *move the money quickly out of the card*, and into other goods/services before the card was cancelled. Instrumental in this quick move was the role of "mules", i.e., people who were involved in accepting and re-shipping goods. Although the people involved in stealing credit card information usually had significant technical expertise, the "mules" usually did not. In some cases, the "mules" did not even know that they were part of a cybercrime business. They thought that this was legitimate employment and that this transfer of money and goods was part of their legitimate job.[410]

57% OF DARK MARKET LISTINGS OFFER DRUGS

Soska and Christin (2015)).

Using this instance (i.e., stealing credit cards) as an example, we can clearly realise why cybercrime has had to evolve and organise as a real business with suppliers, consumers and even offices. In order to make the best profit from these illegal activities (and thus stay below the radar), cybercriminals have involved people from Eastern Europe, the US and elsewhere to ship goods all over the place and to re-sell goods in legitimate markets without alerting any suspicion.

5.12 Drug crime

As drugs[411] are illegal in most places, people who would like to purchase them have turned to the online world. Markets exist (or used to exist) in the dark web where people have been able to purchase drugs under the (relative) safety of anonymity that the dark web provides. Drug sales were a relatively late addition to the cybercrime business as several of the original forums chose to ban any drug sales (along any CSAM material) probably in order to operate "below the radar" and not attract the attention of law enforcement agencies (Lusthaus (2018b)). However, some sites have now chosen to include drugs among their trades and thus are clearly within the "radar" of the law enforcement.

Obviously, there is no doubt that law enforcement should investigate and shut down these sites as needed. Interestingly, although effective cyber-policing might ***reduce*** the volume of illegal

410 https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling

411 In this section we cover trade of illegal drugs. Note that one can also find online drugs which have not been criminalized yet. Such drugs, found under colorful names such as "spice" or "bath salts", since they are legal at the time of their purchase are beyond the scope of this work.

online drugs trade in the ***short term***, it may actually ***increase*** the volume in the long term as cyber-policing victories are publicized and they may lead to "unintended advertisement" of such marketplaces (Lusthaus,(2018b). In addition to this "unintended advertisement", the ***addiction*** that comes with drug use implies that there is a steady demand for drugs (online and offline) that is largely independent from short-term achievements and shutdowns. Indeed, if their (online or offline) source of drugs runs dry, drug users will try to find other places to get their drugs.

With the advent of the dark web, and the anonymity it brings, several marketplaces (and their associated customers) have moved to the dark web.

> ONLINE MARKETPLACES USED A DELIVERY MECHANISM KNOWN AS "NON-CONTACT DRUG DEALING". IN THIS APPROACH, THE SELLER HIDES THE DRUG IN A DRUG STASH (A HIDING PLACE) AND REVEALS THIS PLACE TO THE BYER ONLY AFTER THE TRANSFER OF FUNDS (FROM THE BUYER TO THE SELLER) IS COMPLETE
> Frank and Michaylov.

Examples include the "Dream Market" (Zhou et al., 2020), Silk Road[412], Silk Road 2.0, Alpha Bay[413], Hansa Market[414], etc. Although such markets do not carry only drugs, it has been estimated that 57 per cent of Dark Market listings offer drugs (see Soska and Christin, 2015). Buyers prefer such marketplaces because there is a wider range of drugs, greater convenience, better quality and no physical contact (Bertola, 2020). In a similar spirit, such online marketplaces (i) provide a safer environment for sellers and (ii) give new sellers the possibility to reach clients beyond their geographic region. To protect their anonymity and make it difficult for law enforcement agents to find the parties involved in drug dealing, transactions are paid in cryptocurrency (Btcoin or similar) which provided pseudonymity (or even full anonymity). To protect the anonymity of buyers, Russian online marketplaces used a delivery mechanism known as "***non-contact drug dealing***". In this approach, the seller hides the drug in a drug stash (a hiding place) and reveals this place to the buyer only after the transfer of funds (from the buyer to the seller) is complete (Frank and Michaylov, 2020).

Although most on-line drug transactions happen in the dark web, some of the Russian Marketplaces can be found in the open web through regular web searches. Frank and Muchaylov (2020) report that they were, in this way, able to find 28 Russian online marketplaces for illicit drugs. These market places were not only discoverable on the public web, but they also provided access without registration. After studying these web sites, Frank and Michaylov (2020) reported that they found 935 drug advertisements, some of them (10.3%) for large quantities (i.e., between 3 grams and a kilo) suggesting that these marketplaces cater to wholesale orders as well. Payments were accepted in Qiwi[415] (virtual currency used for personal money transfers and utility bill payments) and in Bitcoin.

[412] https://en.wikipedia.org/wiki/Silk_Road_(marketplace)
[413] https://en.wikipedia.org/wiki/AlphaBay
[414] https://en.wikipedia.org/wiki/Hansa_(market)
[415] https://qiwi.business/en/

5.13 Human trafficking

Human trafficking is defined as "the recruitment, transportation, transfer, harbouring or receipt of persons, by means of the threat or use of force or other forms of coercion, of abduction, of fraud, of deception, of the abuse of power or of a position of vulnerability or of the giving or receiving of payments or benefits to achieve the consent of a person having control over another person, for the purpose of exploitation. Exploitation shall include, at a minimum, the exploitation of the prostitution of others or other forms of sexual exploitation, forced labour or services, slavery or practices similar to slavery, servitude or the removal of organ."[416] Although most of the human trafficking cases are not reported, it is estimated that there are over 45 million victims of human trafficking all over the world (Bonilla and Mo, 2019). Most of these victims are approached through traditional means in the physical world: social circles, neighbourhoods, clubs, bars, etc. About 20 per cent of the victims are approached via the Internet.[417] Perdue reports that most of the trafficked women are recruited online[418]. She describes how traffickers monitor the social media of (usually young) girls in order to find signs of vulnerability. For example, if the girl posts an image in a scanty bikini, this usually implies that there is no adult supervision of her social media accounts. Similarly, if she uses hashtags such as #teenmodel or similar, the trafficker knows that she might be interested in modelling and thus she might be vulnerable to promises of a modelling contract. Even worse, a hashtag named #sexy probably means that the girl is desperate for attention. Armed with this information (i.e., no supervision, vulnerable to promises for a modelling contract, and desperate for attention), the trafficker approaches the girl with a promise of modelling or photoshoot. The trafficker may perform the photoshoot and may even pay the girl in order to gain her trust. Then the trafficker may ask for more revealing photoshoots, etc. leading the girl on a slippery slope that is not easy to get out of. Armed with the revealing pictures, the trafficker starts blackmailing the girl threatening to post the pictures to the media and send them to her family. This, in turn, enables the trafficker to ask for more and more without an end.
In a study of 79 court cases, the United Nations Office on Drugs and Crime reported that, in 31 of them (=39%), there was an element of online advertisement which affected almost half of the total victims.

Terwiller (2021) studied how vulnerable young adults (18-24 years of age) are falling victims to human trafficking through social media. She found that about 43% of them have considered leaving home because they were unhappy. She also found that about 47% of them have sent photos to social media users they do not know and that 45% of the participants have received interest from strangers on modelling jobs or photoshoots.
Although the provision of the services of the victims of trafficking is an "offline" activity, it also has a significant online dimension. Rhodes (2017) reports that the victims of human trafficking are usually forced to sell their services online possibly broadcasting livestream acts of sexual activities.[419] In interviews with trafficking victims, Bouché (2015) reports that half of them were advertised online in places such as Backpage (more than half of them), Craigslist and Facebook.

[416] https://www.ohchr.org/en/professionalinterest/pages/protocoltraffickinginpersons.aspx
[417] https://apps.urban.org/features/theHustle/theHustle.pdf
[418] https://www.psychologytoday.com/us/blog/end-human-trafficking/202107/the-darkest-side-social-media
[419] https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Chapter5.pdf

Backpage started as an ads company – something like Craigslist – and eventually became the second largest website for such ads in the United States.[420] Although Craigslist closed its "adult" section in 2010, Backpage did so only seven years later (2017). In this time interval, several of the adult ads from Craigslist moved to Backpage. A careful investigation revealed that some of these ads were obfuscated human trafficking ads which involved minors. Backpage was used to host advertisements for victims of human trafficking. The United Nations Office on Drugs and Crime studied 79 court cases of human trafficking and reported that in 44 of them (55%) online advertisement was used.
To automatically classify the ads and discover the trafficking-related ones, researchers have started to use machine-learning approaches. For example, Portnoff et al. (2017) report that they can find ads posted by the same author with 90% success rate. Similarly, Lee at al. (2021) suggest that their system can detect ads for human trafficking with 90% accuracy decreasing any manual effort by an order of magnitude.

5.14 CSAM

Although the exact definition of CSAM[421] changes from one country to another, it is illegal in most countries and it quickly attracts the attention of all involved entities: law enforcement, NGOs, politicians, etc. This may be why most of the first profit-driven cybercrime forums (such as CarderPlanet) explicitly prohibited the distribution of CSAM through their websites: distributing CSAM attracts the attention of the police.

5.14.1 How is CSAM distributed online?

The first attempts to distribute CSAM online involved IRC (chat rooms). Carr (2004) reports that back then 78% of CSAM images were acquired from IRCs. Since IRCs could be easily monitored by law enforcement agents, with the proliferation of the Internet, CSAM has moved into other areas online.
For example, in the early 2010s, peer-to-peer systems[422] were popular as a vehicle for distributing CSAM (Wolak, 2014). The main reason is that peer-to-peer systems are versatile and robust in the sense that they (usually) lack a central (web) server: in peer-to-peer systems, every participant acts both as a client and server at the same time. Since they lack a central web server, they are not easy for the policer to shut down; thus, they are a perfect vehicle to distribute illegal material including CSAM. In addition to peer-to-peer systems, lots of CSAM is hosted in the open web through password-protected sites. These sites link CSAM which is usually uploaded in image-hosting sites: sites that provide storage space for users who would like to host their photos and images.
CSAM can also be found in the dark web (see Ligget et al., 2020). Owenson and Savage (2015) studied hidden services[423] on the dark web and report that about two per cent of the "hidden services" in the dark web serve CSAM. This tiny percentage of hidden services corresponds to

[420] https://en.wikipedia.org/wiki/Backpage
[421] Child Sexual Abuse Material – sometimes called CSEM as well.
[422] https://www.europol.europa.eu/cms/sites/default/files/documents/efc_strategic_assessment_2014.pdf
[423] A hidden service in the dark web is the equivalent of a web server in the open web.

80 per cent of the traffic (or more accurately of the requests) among all hidden services, underlying two facts:

- Requests for CSAM are very popular on the dark web, and
- A tiny percentage of services are responsible for most of the CSAM on the dark web.

In addition to delivering images and videos containing CSAM, the Internet has resulted in a new form of (real-time CSAM) cybercrime: "**cyber-trafficking**": that is, child victims of human trafficking are streamed online to customers in different countries. This "cyber-trafficking", since it does not involve the actual physical movement of human beings, is more difficult to detect with traditional means (i.e., ID controls, passports, cameras, etc.) .
Although today the main forms of CSAM consist of images, videos, and live streaming (through cyber-trafficking), it is envisioned that CSAM will move into virtual reality and more interactive virtual worlds.

5.14.2 Where is CSAM located?

Recent studies suggest that CSAM is located mostly in servers in the western world. Indeed, in its 2020 study, the Internet Watch Foundation reported that 90% of the URLs are hosted in Europe (which includes Russia and Turkey), 7% in North America, and the rest is mostly in Asia[424]. We should underline that these stats are for data accessed by the analysts of the Internet Watch Foundation, but still, the results show a trend. With respect to the countries, it seems that the Netherlands host 77% of the URLs, followed by the USA (5%) and France (4%). A few years ago, the situation was completely different. For 2015, IWF reports that only 41% of the reported URLs were hosted in Europe and that close to 57% of the reported URLs were hosted in North America.[425] Thus, we see a trend moving the hosting from North America to Europe.

5.14.3 Business model

Although most of the CSAM images are served for free in (initially) peer-to-peer systems and more recently on the web (including the dark web), it is estimated that up to 18% of them are being sold fueling a profit-driven market (Ligget (2020)). Prices vary widely from 10 USD per video download to 50 USD for a monthly subscription. To protect their anonymity, customers use PayPal or bitcoin. Forums in the dark web frequently mention web sites that contain CSAM and are reported in hotlines (Kokolaki et al. (2020)). Recent reports suggest that in an increasing number of cases the material is produced in the child's home by an adult relative or even a parent.[426]
Some of the material is produced by the underage people themselves (mostly teenagers). The Internet Watch Foundation reports that, in as many as 44% of their reports, the content was

[424] https://annualreport2020.iwf.org.uk/trends/international/geographic
[425] https://www.iwf.org.uk/media/iqqdc3sf/iwf-2017-annual-report-for-web_0.pdf
[426] https://ecpat.org/wp-content/uploads/2021/05/ECPAT-International-Report-Trends-in-Online-Child-Sexual-Abuse-Material-2018.pdf

self-generated.[427] Although this content may be content by teenagers who were tricked or blackmailed to generate it, there are cases where teenagers generate this content for their own profit. See, for example, the case of Justin Berry as reported in Westlake (2020).

5.15 Online harassment - cyberbullying

FOUR IN TEN AMERICANS HAVE EXPERIENCED ONLINE HARASSMENT
Duggan (2017)

Although harassment existed well before the digital age, it has proliferated with our increased use of the Internet. As a result, a large number of people has started to experience online harassment. For example, Duggan (2017) reports that "41% of Americans have been personally subjected to harassing behaviour online, and an even larger share (66%) has witnessed these behaviours directed at others". Wilsem (2013) found a much lower percentage of people who have experienced online harassment – but this is possibly due to the fact that different definitions of on-line harassment may exist. Wilsem suggested that "Higher risk of harassment victimization were documented for those engaging for long periods of time on Internet communication activities, such as forums, e-shops, social networking sites, and webcams. This means that chances of being harassed online were not dependent on one's skills or knowledge of computer safety nor from the use of computer security measures." However, some precautions always help. Indeed, Moneva et al. (2021) suggest that students who restrict access to their social media profiles are among the least likely to report being repeatedly victimized. At the same time, the profiles most likely associated with online harassment are defined by students who allow other users to access their profiles. Thus, restricting access to media profiles seems like a good idea.

Although some of these harassment experiences can be considered to have a low impact, "one-in-five Americans (18%) have been subjected to particularly severe forms of harassment online, such as physical threats, harassment over a sustained period, sexual harassment or stalking." Although people get harassed for a wide variety of reasons, political views, physical appearance, ethnicity and gender seem to top the list.

|In this age of social media, the issue of online harassment is widely known and clearly seen. What is less clear, however, is what needs to be done about it. Indeed, some people see that curbing on-line harassment might interfere with freedom of speech. Duggan (2017) reports that roughly half of the Americans say it is more important to let people speak their minds freely online, while the other half believe that it is more important for people to feel welcome and safe online.

What people seem to agree on is that the Internet allows for anonymity. Duggan (2017) reports that 86% of online adults feel that the Internet allows people to be more anonymous which may lead to harassment. Half of those who have been harassed online (54%) say their most recent incident involved a stranger and/or someone whose real identity they did not know. Social media (and the Internet) seem to support this anonymity (or at least pseudonymity). Most online

[427] https://annualreport2020.iwf.org.uk/trends/international/selfgenerated

harassment targets say their most recent experience occurred in a single venue, often social media.

Hinduja and Patchin (2014) define cyberbullying as "willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices". Offenders frequently use electronic means including mobile phone and social media. These enable them to perform cyberbullying 24/7 sometimes in front of a large audience that may amplify the effects of bullying. Barlett et al. (2018) suggest that "social networking can be used to harm others through the development of positive cyberbullying attitudes—a link that has received very little empirical attention."
Navarro and Marcum (2020) suggest that cyberbullying occurs mostly among young adolescents. This is the time when peers assume a great effect as a socialisation agent. During this period "one's reputation among their peers is an extremely important form of social capital. Youth may perform acts of cyberbullying to assert their status or recover from being a bully themselves". At this age, "association with deviant peers and favourable beliefs toward cyberdeviance increased the odds of perpetrating cyberbullying".
Oksanen et al. (2020) report that cyberbullying is also prevalent at work. Indeed, they report that cyberbullying is prevalent in almost 18% of the Finish population. They report that victims were more commonly young, men, and had a lower level of education. They also report that cyberbullying is a predictor of psychological stress and work exhaustion. Interestingly,h they did not find any major differences between occupational fields, indicating that cyberbullying at work concerns workers in a variety of fields.
Given that online harassment and cyberbullying does not need any elaborate technical infrastructure (such as dark web) or capabilities, people have started to propose automated detection approaches in social media – where most of harassment is taking place (see Kennedy et al., 2017).

5.16 Extortion – sextortion

Extortion is the act of obtaining money or property by threat to a victim's property or loved ones, intimidation or false claim of a right (such as pretending to be an IRS agent).[428] Ransomware (section 8.2.1) is a form of extortion. Attackers encrypt all files of the victim and demand money (usually in difficult-to-trace cryptocurrencies) to decrypt the files. Victims who do not have any other ways to find their files (e.g., through a back-up or a second copy) are frequently forced to pay the money demanded.
To implement this ransomware-based extortion, attackers need to find a vulnerability in the victim's computer so as to compromise it and install the ransomware. If no such vulnerability is found, sometimes the victim is tricked (usually via social engineering) to install the ransomware themselves. We must underline that, once ransomware is installed, it is capable of inflicting even more serious damage including permanently deleting all files, changing the user's passwords, stealing confidential information, etc.

In addition to requests for money, extortion in cyberspace may include demands for other things including sexual photos and favours. In this special kind of extortion, called "sextortion",

[428] https://dictionary.law.com/

cybercriminals get some important or private information about their victims. Then, the cybercriminals request explicit photos from the victims in order not to release the said information. When the cybercriminals get the explicit photos, they become more aggressive and request even more: favours, money, videos, etc. In some other cases, the cybercriminals set a trap, which is usually a video of a woman through which they convince the victims (usually males) that the video is real-time performance and encourage them to undress. Once the victims fall in this trap, the cybercriminals record the victims and then try to extort money from them.[429]
Some cybercriminals manage to take control of the victim's computer and activate the webcam. In this way, they record the victim and use these recordings for sextortion (Andrews et al., 2015). Recently some cybercriminals engaged in sextortion without even having any photos of the victims. The cybercriminals pretend to have such photos (or videos) and threaten that they will publish them unless the victim pays some money. To "prove" that they have such photos, cybercriminals may present the victim with his/her password. The password was usually found in some data leak and was for a website completely unrelated to the victim's home computer. Nevertheless, the attackers showed that they had some private information about the victim (i.e., the password), claimed that they had much more private information (i.e., explicit photos) and demanded money (Nussabum and Udon, 2020). [430]
Although sextortion can cause serious trauma, prosecution of sextortion has been effective mostly in cases where the victims are minors. In cases where the victims are adults, charging is not very effective and has to resort to creative approaches due to gaps in the legal systems (see Wittes et al., 2016, and Holt and Lidget, 2020).
Sextortion against minors seem to have different dynamics. In a survey, Wollak et al. (2018) reported that more than 60% of the victims knew the perpetrators often as romantic partners. To provide the explicit images, about a third of the victims were threatened with physical assault. Most of the victims (91%) were female in the age group 16-17 (75%).

5.17 Grooming

Bishop (2020) suggests that "While there is no universally accepted definition of grooming, the term is generally used to describe the process by which a person engineers a relationship with a child in the hope of gaining the child's trust prior to some form of sexual contact." Although grooming is not a new phenomenon, the Internet has given rise to online grooming. The anonymity that the Internet provides enables cybercriminals to approach potential victims while hiding their real identity. In any case, since grooming is a first step in a long line of steps that lead to criminal behaviour, it has been studied widely.
For example, Montiel et al. (2016) in a study of 3,897 adolescents between 12 and 17 years old, found that 17.2% have experienced grooming by an adult. The percentage is higher for females (24.2%) than males (9.4%). The percentage was also higher for the higher age groups: 25.6% for the age group 16-17. Although the percentages are alarmingly high (one out of four adolescents being cyber groomed), some of these attempts may not have been successful. Unfortunately, Wachs et al. (2012) report a similarly high percentage in Germany: 21.4% of

[429] https://www.thesun.co.uk/news/2293628/sextortion-how-common-is-webcam-blackmail-and-how-to-keep-yourself-safe-online-latest/
[430] https://www.eff.org/deeplinks/2018/07/sextortion-scam-what-do-if-you-get-latest-phishing-spam-demanding-bitcoin

the adolescents surveyed (aged between 12 and 16) has been in contact with a groomer they had met online: 10.4% reported of online solicitation once a year, 4.3% once a month, 1.9% once a week, and 4.6% of the participants several times a week. Since lots of young children have access to the Internet, online grooming is easier (Whittle et al., 2013). Other factors such as gender (girls are more likely to be victims), age (younger teenagers are less likely to encounter online grooming compared to older teenagers), and trouble with school, all contribute to adolescents being victims of online grooming (Whittle et al., 2013b).
De Santisteban et al. (2018) studied the process cybercriminals use for online grooming. Using information from 12 men convicted for online grooming, they show that the process follows these steps: (i) they establish the Internet as a place where they can express themselves – a game changer, (ii) they try to gain access to several minors at the same time, (iii) they persuade the victims by creating a fake personality (age, education level, etc.), (iv) they become interested in the victim's environment (e.g., parent supervision, happiness at home, etc.), and (v) they adopt a strategy that suits the victim. For example, in some cases, they use deception, in other cases, they use bribery (money, tickets, VIP passes, etc.), and in still other cases, they use aggression (intimidation, extortion, etc.).
Given the importance of early detection, recent research has developed automated approaches to detect grooming behaviour in social media. For example, Anderson et al. (2020) describe an AI-based approach able to detect online grooming with close to 60% accuracy. Similarly, Ngejane et al. (2018) report on automated systems that are able to achieve accuracy of close to 90%. Although different systems use different training data and, thus, may have different performance, using AI to automatically detect some of the online grooming conversations has encouraging results.

5.18 Revenge porn

Holt and Ligget (2020) report that revenge pornography has been used to refer to the "unauthorized use, distribution, or publication of sexual images that were either sent consensually or obtained without the permission of the victim through hacking or unlawfully accessing the victim's personal data." Two are the main dimensions of revenge porn: (i) the distribution of images is done without the victim's consent and (ii) there is an element of revenge in this distribution. Distribution of such images usually takes place via the Internet through dedicated websites or similar forums. The actual number of such websites is not known, butis estimated to be in the few thousand.
Most victims are female (Holt and Ligget (2020)), although minorities from the LGBT community are victims as well. Revenge porn is a form of abuse, like sextortion, with one major difference: revenge porn usually happens in public (i.e., by uploading the images of the victim to a site accessible by lots of people). In this way, the cybercriminal tries to publicly humiliate the victim. The public nature of this crime usually makes it difficult to stop it. Indeed, although images may be uploaded initially to one website, they may be uploaded to other websites too leading a a constant process of victimization. As a result, it is difficult to take those pictures down from all places in cyberspace.
Revenge porn, or at least the path that leads to it, is widespread. Lenhart et al. (2016) report that "roughly 3% of all online Americans have had someone threaten to post nude or nearly nude photos or videos of them online", and that "2% of online Americans have had someone actually post a photo of them online without their permission". This means that roughly one

out of 25 online Americans "have either had sensitive images posted without their permission or had someone threaten to post photos of them". If we focus on women or minorities, these percentages are even higher. For example, about 10% of women ages 15-29 have had someone threaten to expose photos of them. For the LGBT community, this increases to 15%. A more recent study by Ruvalcaba et al. (2019) reports that 8% of the participants reported at least one instance of nonconsensual pornography victimisation in their lifetime. When we consider gender and sexual preferences, the percentages are high for women and minorities. For example, the percentage for heterosexual women was 6.74% and for bisexual women 17.19%. The study showed that men can be victimised as well: heterosexual men (5.63%) and bisexual men (12.82%). The same study also focused on perpetration rates by asking the following question: "Have you ever knowingly shared a sexually explicit image or video of someone else without his/her consent?" The results were impressive: 5% of the participants admitted that they had shared such images. The percentages were higher among men: bisexual (11.11%), gay (10.83%), and heterosexual (6.37%). However, the study also showed that women were also perpetrators: 2.66% of heterosexual women admitted to having shared such material. The percentage was higher for bisexual women (4.95%) but lower for lesbians (1.41%).
From a technical point of view, revenge porn is a cybercrime that does not need an elaborate technical infrastructure. Indeed, the perpetrator knows the victim (intimately), takes the pictures using commodity technology (such as a smartphone), and later uploads the offending material to a website (usually on the public web). From a technical point of view, the perpetrator does not need any sophisticated knowledge. It seems however, that technology may bring harm in more ways than one, and several scholars consider revenge porn as an instance of a broader set of crimes that fall under the term "image-based abuse" (Henry and Flinn, (2020).

5.19 Hate speech

Although there are several definitions for hate speech, Costello and Howdon (2020) define hate speech as "the use of computer technology or digital platforms to express hatred toward a collective identity on the basis of race, ethnicity, gender, gender identity, sexual orientation, national origin, religion, or other group characteristic". This does not mean that hate speech can not target individuals. But in these cases, the victim is targeted because of his/her characteristics (such as race, gender, etc.).
Different jurisdictions criminalise different behaviours of hate speech. Such criminalisations usually have in common the following: (i) hate speech is targeted towards a group or towards the properties of a group (and towards an individual), and (ii) they may include some form of violence (or encouragement to violence).
Hate existed well before the advent of the Internet. However, the Internet made it easier for people (i) to find others with similar ideas and (ii) to express their hate speech against other groups. It started with Internet bulletin boards (Becker et al., 2000), then moved into Usenet groups (Pollock, 2009), and eventually into social media and publicly accessible websites. Since speech on the Internet is not easy to censor or regulate, several groups use the Internet to disseminate hate speech. For example, hate groups have been using the Internet from its early days in order to organise in groups, find new members and disseminate hate speech. The

Internet is so useful that some people state that "The Internet is our battleground!"[431] The Internet (and online social media) help in the organisation of hate groups through announcements, posts, mass mails, etc. At the same time, the distance and the "anonymity" provided by the Internet allows haters and hate groups to build a persona that feels "interesting" or even "edgy" (Costello and Hawdon, 2020) encouraging hesitant bystanders to follow this culture of hate.

As a result, online hate is widely prevalent today, as reflected in several studies. Costello et al. (2016) surveyed 1034 Internet users aged 15 to 36. They report that the majority (65.4% to be exact) of them saw or heard hate material online in the prior three months. They said that in about 20% of the cases the material called for violence or discrimination against the targeted group. The most frequent properties targeted by hate included race (46.3%), sexual orientation (33%), religion (27.3%) and nationality or immigration status (20.7%). The most frequent venues in which they encountered hate speech included Facebook (47.6%), Youtube and Twitter. More recent studies show an even larger percentage of exposure to hate speech. In their study a couple of years later, Hawdon and Costello (2018) report that exposure to hate speech had increased to 72.7%. According to a Eurobarometer study, 75% of Europeans have witnessed hate speech directed at journalists, bloggers and people on social media. [432]

These large percentages may be due to the fact that hate speech reaches popular (social) media and that people spend more time on such media.

Hate speech online is harmful to its victims for a long time after it is originally posted. Indeed, posted material in social media and websites is usually not deleted, and stays there for months or years. In this aspect, it causes harm in a continuous and sustained way. To make matters worse, the harm is caused even if the perpetrator and the victim never interact with each other. Online filtering or "preferences" algorithms may actually amplify this effect. Indeed, some websites use algorithms to display news that fit the users' interests, preferences and past accesses. As a result, users may be trapped inside a "hate-speech bubble" where they see again and again articles related to hate speech leading to a vicious circle that they can not easily get out of.

5.20 Cyber terrorism – violent extremism - radicalisation

Much like other aspects of cybercrime, there is no single universal definition of cyber terrorism. Akhgar et al. (2014) define it as the "convergence of cybernetics and terrorism". Denning defines it as "the convergence of terrorism and cyberspace. It is generally understood to mean unlawful attacks and threats of attack against computers, networks, and the information stored therein when done to intimidate or coerce a government or its people in furtherance of political or social objectives. Further, to qualify as cyberterrorism, an attack should result in violence against persons or property, or at least cause enough harm to generate fear".[433] Weinmann suggests that cyber terrorism is "the use of computer network tools to harm or shut down critical national infrastructures (such as energy, transportation, government operations)". Although some definitions are narrow and some are broad, we see that (at least both Denning's and

[431] https://www.pbs.org/independentlens/blog/who-is-watching-the-hate-tracking-hate-groups-online-and-beyond/

[432] https://ec.europa.eu/information_society/newsroom/image/document/2016-47/sp452-summary_en_19666.pdf

[433] https://irp.fas.org/congress/2000_hr/00-05-23denning.htm

Weinmann's) they focus on the impact of the result: e.g., cause harm, shutdown critical infrastructures, etc. A survey of the various definitions can be found in Pltonet et al. (2021) who proposes a new definition: "Cyber terrorism is the premeditated attack or threat thereof by non-state actors with the intent to use **cyberspace** to cause **real-world consequences** in order to induce **fear** or coerce civilian, government, or non-government targets in pursuit of social or ideological objectives. Real-world consequences include physical, psychosocial, political, economic, ecological, or otherwise that occur outside of cyberspace."
Although cyberterrorism is an issue that concerns all people, there is very little information about it. Scivens et al. (2020) suggest that "Reviews of the terrorism research literature regularly highlight the paucity of original data that inform analyses" and recommend to make "Archives of Violent Extremist Online Content Accessible for Researchers".

Cyber terrorists use the Internet for recruiting new members. Berger and Morgan (2015) analyse a sample of 20,000 twitter accounts that support ISIS (Islamic State of Iraq and Syria). Their results suggest that between September and December 2014 more than 46,000 accounts were used by ISIS supporters. They found that "ISIS-supporting accounts had an average of about 1,000 followers each, considerably higher than an ordinary Twitter user" and that "ISIS-supporting accounts were also considerably more active than non-supporting users". They also found that "much of ISIS's social media success can be attributed to a relatively small group of hyperactive users, numbering between 500 and 2,000 accounts, which tweet in concentrated bursts of high volume".[434] Speckhard and Ellenberg, through interviews with ISIS fighters, show that Internet recruitment alone has been enough to convince some people to leave their home countries in Europe and join a terrorist group. In doing so, they show the power of the Internet in terrorist recruitment.
Conway (2006) suggests that cyberterrorists also use the Internet to promote their cause and to provide information (in text, images, and videos) to a mass audience (usually) without any (immediate) form of censorship. Such information may be used to intimidate and instil fear to the general public. Conway (ibid.) also suggests that terrorists use the Internet to raise funding for their activities. Such funding can be raised through direct donations, purchase of items/services, and more recently through (anonymous) cryptocurrencies (Teichmann, 2018; Majumder, 2019; Amiram et al., 2020).

5.21 The gender dimension

Several studies explore how gender may have an impact on cybercrime. Such studies explore the following two questions:

- Are people of a particular gender more likely to be cybercrime perpetrators?
- Are people of a particular gender more likely to be cybercrime victims?

There does not seem to be a simple (or single) answer to the above questions. ***In some cases, males are more likely to be perpetrators*** and in others, both genders are (almost) equally likely. It seems that the type of cybercrime may play a leading role in whether it is male-dominated or not.

[434] https://apo.org.au/node/53568

Similarly, in some cases of cybercrime victims, females are more likely to be victims and in other cases, both males and females may be victims of cybercrime without any noticeable gender difference. For example, financial-related cybercrime (e.g., fraud, phishing, etc.) seems to target both males and females equally. On the other hand, for harassment or abuse-related cybercrime, females are more likely to become victims. The next two subsections explore the gender dimension in more detail.

5.21.1 Perpetrators

Both males and females are involved in cybercrime as perpetrators. The actual percentages differ depending on the type of cybercrime (and the study itself). For example, published results from the Cambridge Computer Crime database[435], as reported by Lusthaus (2018b), suggest that males dominate cybercrime. Males are involved in 93% of malware attacks, in 80.3% of data (or systems) breach attacks, in 100% of DDOS attacks, in 84.1% of fraud/phishing attacks and in 74.2% of money laundering attacks. Based, in part, on similar data, Hutchings and Chua (2016) report that "very few cybercrimes are committed by females". Their results suggest that although females are engaged in cybercrime, they are more involved in "general" crimes and less involved in "technical" crimes. Also, when involved they are usually not the primary offender and engage in less serious activities. One possible reason for that is the "lack of female involvement in crime in general, compounded with the gender gap found in the computer sciences". We should note, however, that their study does not include cybercrime of an interpersonal nature such as CSAM, cyber stalking, online harassment, as well as online piracy and counterfeit products.

In the area of cyberstalking, Dreßing et al. (2014) suggest that 69% of the cyberstalkers were male and MacFarlane and Bocij (2003) suggest that the percentage of male cyberstalkers was as high as 84%. When considering other kinds of cybercrime where financial motive is not the main driver, the traditional balance between males and females seems to change. Lusthaus (2018b) reports that females are more frequently engaged in cashing out profits from stolen credit cards. For example, they use stolen credit cards to purchase goods and they receive stolen merchandise in their physical addresses via postal services.

In human trafficking, most (convicted) offenders (64%) are male, while the rest 36% is female.[436] Female offenders are more involved in the initial stages of trafficking, e.g., in the recruitment phases. Since the initial stages may happen at the country of origin, the statistics for the (convicted) offenders may change: In countries of origin of human trafficking, we see more female offenders – up to 80% in Eastern Europe and Central Asia.

[435] https://www.cl.cam.ac.uk/~ah793/cccd.html
[436] https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Global_overview.pdf

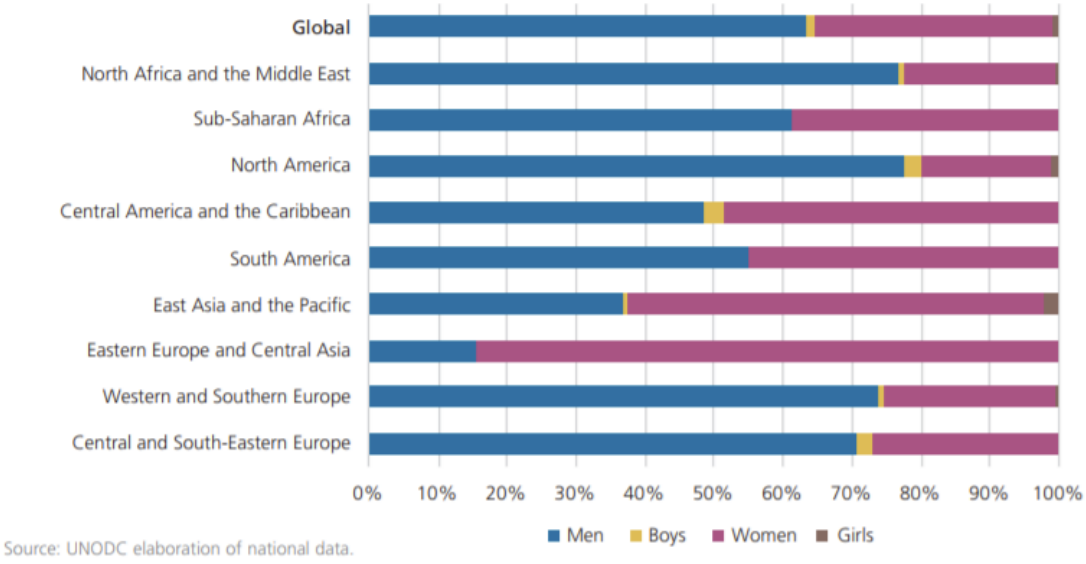


Figure 11: Percentage of convicted offenders for Human Trafficking. We see that in overall (Global – first bar) 64% are male and 36% are female. Source: UNODC, Global Report on Trafficking in Persons 2020 (United Nations publication, Sales No. E.20.IV.3).

5.21.2 Victims

Schreuders (2019), based on police data from the UK, reports that "females were much more likely to become cybercrime victims than males for two types of cybercrime: "Harassment/Unwanted contact" and "Sexual/Indecent Images". However, both males and females were vulnerable to "Fraud/Theft/Handling" cybercrime. Strawhum et al. (2013) report that women admitted greater frequency of cyberstalking perpetration than males. Berry and Bainbridge (2017) reported that, contrary to offline stalking, "males were as likely to be cyberstalked as females". Moreover, males may suffer even more severe consequences when cyberstalked by female ex-partners as reported by Kaur et al. (2021). Ahlgrim and Terrance (2018) report that the male victims were blamed more for the occurrence of cyberstalking behaviour and that their claims as a victim were taken less seriously and perceived as less legitimate. On the contrary, female victims were attributed less blame than male victims. Although in the area of cyberstalking, some studies suggest that females are the majority of victims (68.75% as reported by Fansher and Randa, 2019), the gap between males and females is smaller.
In the area of online harassment, Duggan (2017) reports that "men are somewhat more likely to experience 'any' form of harassing behaviour online", and that "men are modestly more like to have been called offensive names and to have received physical threats". However, women "encounter sexualized forms of abuse at higher rates than men" and especially in the age group 18-24 where women are three times more likely to be sexually harassed online than men.

In the area of human trafficking, statistics from the United Nations suggest that 46% of the victims seem to be women, 20% men, 19% girls, and 15% boys. [437] The results suggest that most women and girls were trafficked for sexual exploitation where men and boys were trafficked mostly for forced labuor. In the area of online CSAM, girls are the main victims. The

[437] https://www.unodc.org/documents/data-and-analysis/tip/2021/GLOTiP_2020_Global_overview.pdf

IWF reported that girls appeared in more than 90 per cent of the images processed by their analysts.[438]

5.22 The geographical dimension of cybercrime

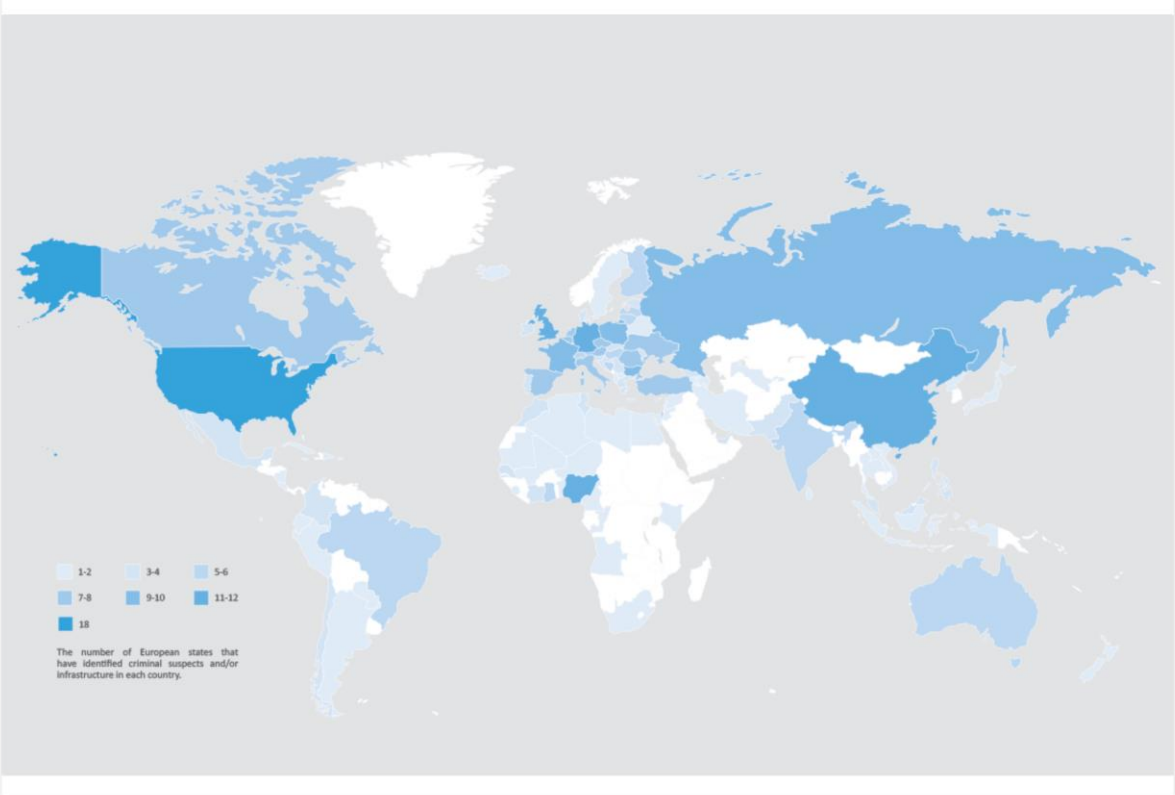


Figure 12: Map of Cybercrime. The map shows the "number of European States which have identified criminal suspects and/or infrastructure" in each country. Darker colors mean that more European States have identified criminal suspects in this country. We see that the countries that top the list are Nigeria, China USA, and Germany. Significant roles are also played by Russia, Canada, India, Australia, Brazil, etc. Source: Europol https://www.europol.europa.eu/iocta/2016/resources/iocta-2016.pdf

Although cybercrime is global phenomenon, it has clear geographical dimensions. Specific geographic regions may specialise in some aspects or others. For example, countries of the former Soviet Union have been effective in malware production and distribution (Lusthaus, 2018b). Russian-speaking individuals have organised around online forums to collaborate and be more effective. CarderPlanet was one of the first such high-impact Russian-speaking forums. After CarderPlanet was closed, several other Russian-speaking forums emerged including Mazafaka, Verified, Direct Connection, anti-chat.ru, and reversing.net (Lusthaus 2018b). People in the West (such as North America and Europe) have been more suitable for cashing out (e.g., using stolen credit cards) and in money mules (e.g., transfer of illegal funds). The

[438] https://annualreport2020.iwf.org.uk/trends/international/overview

following subsections focus on cybercrime in particular areas including ex Soviet Union, Nigeria, China, South America, China and India.[439]

5.22.1 Russia ex Soviet Union

Lusthaus (2018b) reports that some of the first individuals engaged in cybercrime originated from Russia or from the broader area of the ex Soviet Union. There can be several reasons for this. For example, Lusthaus (2018b) suggests that the solid education in STEM (Science, Technology, Engineering and Math) subjects resulted in individuals who had the technical expertise to engage in hacking. As a result, several forums were created by Russian-speaking people including carder.su, CarderPlanet, Mazafaka, etc. The forums were used (i) to make contacts, and (ii) to sell/purchase necessary goods and services. Kadlecová (2015) suggests that "there is not one single prevailing factor behind the dominant position of Russian-speaking cybercrime", proposing that "the online illegal activity has its roots in the 1990s and early 2000s supported by a power vacuum, high unemployment of technically educated individuals and a promising financial return". Finally, she suggested that "weak penalties and legal loopholes in the Russian Criminal Code further motivate criminal organizations in their activities".

Frank and Michaylov (2020) recently reported that illegal activities (such as online drug dealing) has moved to the public web, as they were able to find on the public web (not the dark web) 28 Russian online marketplaces for illicit drugs. Russian-speaking sites seem to have pioneered a novel approach to online "**non-contact**" **drug dealing.** Non-contact drug dealing is done in complete anonymity without any physical contact between the buyer and the seller. Indeed, the advertisement of the drugs is done online, the order of the drugs is done online, the payment of the drugs is made online and the final delivery of the drugs is done in a "***drug stash***", instructions to which are given online to the buyer after the payment is received. This approach provides protection (from the police) not only for the buyer (who does not provide any delivery address for the delivery of goods), but also for the seller who avoids falling in any "buy and bust" operations by undercover police agents.

Russian press and websites are regularly report on the extent of cybercrime in the country. For example, χακερ.ru[440] is a Russian website and magazine that publishes hacking tutorials and news about cyberattacks and information security. The domain has been active for 23 years and the identity of the owner is still hidden. It provides subscriptions where the user (i) can gain full access to hacking manuals, guides and software[441] and (ii) can attend coding courses and training[442]. xakep.ru has reported on cybercrime trends in Russian for more than 15 years. For example, an article from 2005[443] reported that cybercrime incidents doubled each year compared to a modest increase of 15-25% in 2005 where only 13,000 cybercrimes announced by the Russian Ministry of Information and Communication. A possible explanation for the increases was the increase in the efforts of law enforcement agencies and the fact that Russian hackers were entering at the international level, thus being less exposed in Russia. In another

[439] We should note, however, that a review aiming to map the geography of cybercrime by Lusthaus et al. (2020) argues that quality research in this area is still very limited and sparse. The mapping itself exhibits several issues related to the difficulty of identifying locations from where cybercrime originates.

[440] https://xakep.ru/

[441] https://xakep.ru/about-magazine (in Russian)

[442] https://my.xakep.ru/courses/ (in Russian)

[443] https://xakep.ru/2005/03/04/25774/ (in Russian)

more recent article, xakep.ru presents a categorisation of the cybercrimes that were reported in Russia during the year 2019[444]. ATM hacking, carding, phishing and ransomware were the dominant cybercrimes. Other articles present the situation of cybercrime in Russia during the COVID-19 pandemic[445]. Allegedly, the consequences of the pandemic, the transfer of employees to remote work, staff reductions and the financial crisis caused a rapid increase in computer crime. Particularly, for the period from January to June 2020, according to the Russian Ministry of Internal Affairs, the growth in cybercrime amounted to 91.7% compared to the same period last year while traditional crimes decreased. Similar to xakep.ru is **securitylab.ru** which has many articles and material about hacking, cyber threats and cybercrime[446,447]. Moreover, the "as-a-service" business model in the domain of cybercrime, described in detail in this document, is regularly analysed in articles from securitylab.ru[448] as well as other popular Russian general-content news websites[449,450].

Russian media also report on the situation of cybercrime beyond the country by bringing to their readers interesting news about information security and hacking. For example, some recent articles in the news section of xakep.ru concerned:

- **Attacks** (e.g., (i) the cyber-attacks on cryptocurrency platforms that were executed by North Korean hackers who managed to steal almost US$400 million[451] (ii) a DDoS attack of a magnitude of 3.47 Tb/s repelled by Microsoft's DDoS protection platform in December 2021. The attack targeted an Azure customer in Asia.[452]
- **Malware** (e.g., a new ransomware family called White Rabbit, which is operated by the FIN8 hacker group, executed an attack on a local US bank in December 2021[453]. Moreover, a new version of the BRATA Android malware, which was initially active in Latin America in 2019, is currently operating in Europe. This version steals banking information, tracks the location of the victims and finally resets all device settings to remove traces of the malicious activity[454]).
- **Underground market places** (e.g., UniCC, a leading dark web marketplace of stolen credit cards, stopped operations. UniCC has been active since 2013 and has received cryptocurrency payments of more than $350 million US[455]).
- **Hack groups** (e.g., a report on the infrastructure, tactics and techniques used by the Chinese hack group Earth Lusca that has attacked various targets, including government

444 https://xakep.ru/2020/06/23/criminal-cases-2019 (in Russian)
445 https://xakep.ru/2020/10/23/covid19-crimes/ (in Russian)
446 https://www.securitylab.ru/analytics/528719.php (in Russian)
447 https://www.securitylab.ru/blog/company/AngaraTech/350166.php (in Russian)
448 https://www.securitylab.ru/news/517005.php (in Russian)
449 https://business-magazine.online/fn_52695.html (in Russian)
450 https://plusworld.ru/journal/2021/plus-2-2021/kiberprestuplenie-kak-usluga-vliyanie-caas-na-landshaft-ugroz-v-oblasti-ikt/ (in Russian)
451 https://xakep.ru/2022/01/14/dprk-stast/ (in Russian)
452 https://xakep.ru/2022/01/27/new-ddos-record-2/ (in Russian)
453 https://xakep.ru/2022/01/19/white-rabbit/ (in Russian)
454 https://xakep.ru/2022/01/24/new-brata/ (in Russian)
455 https://xakep.ru/2022/01/17/unicc-closed/ (in Russian)

agencies, educational institutions, media, research organizations, telecommunication companies, religious movements[456], etc.)

- **International operations and police arrests** (e.g., the Nigerian Police Force (NPF) joined forces with INTERPOL and arrested 11 cybercriminals including members of the SilverTerrier BEC group (aka TMT), which exists since 2019[457]).

5.22.2 Nigeria

Individuals from Nigeria have been involved in cybercrime activities usually called the "Nigerian letter"[458] or the "Nigerian Scam". These activities started in the 1980s (Lusthaus, 2018b) using regular mail and physical letters delivered by the post office. In this scam, potential victims received a letter informing them about a large amount of money in their name (for example, an inheritance, a donation, or even charity money). However, in order to receive the funds, the potential victims needed to provide a small amount of money for processing fees (or even to bribe corrupted officials who did not want to release the money). With the proliferation of the Internet, such scams moved to cyberspace where potential victims were approached by email, SMS and phone: cheaper, faster and in larger scales (Aneke et al. (2020). Adesina (2017) links this "Nigerian letter" (and other cybercrime activities) to poverty and unemployment in Nigeria, stating that "Nigeria's rising cybercrime profile may not come as a surprise, considering the high level of poverty and high unemployment rate in the country." Interestingly, some believe that this kind of poverty really justifies cybercrime. Olofinbiyi (2021) indicates that while some youths condemned outrightly the involvement in cybercrime, others embraced it as a coping strategy for the Nigerian youth who are unemployed, frustrated and deprived of socio-economic needs.

Although the "Nigerian letter" family of scams has been widely distributed, there does not seem to be behind it a hierarchy reminiscent of organised crime (Lusthaus, 2018b). Instead such scams seem to be operating from small groups of people with loose ties.

Another, recently discovered, Internet fraud ran through dating apps and targeted women in the United States. In this scam, the victims believed that they had a romantic relationship with a person from South Africa. The conspirators used dating sites and social networking platforms to lure their victims. After a while, such a person, who was falsely traveling to South Africa for work, needed money after a series of unfortunate events in his life. The victims of this sexual fraud were convinced to send money and valuables abroad to help this person. In cases where the victims hesitated to provide financial help, the conspirators used manipulative tactics to force payments, including threatening to publish personally sensitive photos of the victim. For these cybercrime activities, eight Nigerian men were arrested and accused of wire fraud conspiracy and money laundering of $7million US[459].

[456] https://xakep.ru/2022/01/18/earth-lusca/ (in Russian)
[457] https://xakep.ru/2022/01/19/silverterrier-bec/ (in Russian)
[458] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/nigerian-letter-or-419-fraud
[459] https://www.bbc.com/swahili/habari-58991137 (in Swahili)

5.22.3 China

China has attracted a lot of attention for government-supported cyberespionage (Lusthaus, 2018b) and cyberattacks. On the other hand, more traditional, individual-based, profit-driven cybercrime seems to be of lesser concern. Copyright-infringement and on-line gaming issues have been reported (Lusthaus, 2018b). As a result, the spread of cybercrime in China is more limited compared to other countries. Although there are several theories for that, more research is needed. Ronggong and Lijia (2020) and Genlin and Baker (2020) describe the cybercrime-related legal system in China which (i) requires more data collection from ISPs, (ii) enables better crime attribution, and (ii) possibly deters cybercrime against targets in China. Another theory is that the language barrier between the English-speaking western world and the Chinese-speaking people in China may inhibit the propagation of cybercrime (Lusthaus 2018b). Whatever the reason, we did not see in China the profit-driven cybercrime backed Since 2020, however, things have started to change and we are starting to see lots of profit-driven attacks. For example, Xinhuanet.com, a news agency with a network of 10,000 journalists, shows the recent situation in the country and states that the number of cybercrime cases has risen from an average annual rate of nearly 40%, to 54% in 2020[460]. Among all cybercrimes, online fraud and online gaming and gambling (including the crime of opening a casino and the crime of gambling) are running at a high level, becoming one of the main types of current cybercrime. For instance, a popular cybercrime in China involves scammers' use of online dating apps to build fake love relationships as bait to deceive victims into committing false investments and money transfers. Such love scams, similar to those from the Nigerian cybercriminal groups, are commonly known as "*sha zhu pan*" in Chinese, or "pig butchering" in English. A year later, in 2021, the Chinese police investigated and handled 62,000 cybercrime cases including personal information infringement and hacking. For these cases, 103,000 suspects were arrested and 27,000 Internet firms and institutions received administrative penalties[461].
From a national perspective, a report from the Supreme People's Procuratorate, the highest national agency responsible for legal prosecution and investigation in China, states that many cybercrime cases are successfully identified every year and that in 2020 about 140,000 cybercriminals were prosecuted[462]. The same report describes the complexity in investigating cybercrime cases and the challenges faced by LEAs in handling such cases. In many cases, the need for technical knowledge to handle the cases overwhelms the need for legal skills. For such reasons, in 2020, the Supreme People's Procuratorate was planning to set up a research steering group to enhance the security in the national cyber space and strengthen the forces in the fight against cybercrime[463].

5.22.4 South America

Lusthaus (2018b) suggests that Brazil plays a leading role in cybercrime in South America, a factor of which may be Brazil's relatively well-developed financial sector (Kshetir and DeFranco, 2020). Thus, the focus of cybercriminals in Brazil has been the local market specialising in credit card fraud and banking fraud. The targets have mainly been Brazilian

[460] http://www.xinhuanet.com/legal/2021-01/25/c_1127024206.htm (in Chinese)
[461] http://www.news.cn/2022-01/05/c_1128235776.htm (in Chinese)
[462] https://www.jcrb.com/rmjc/xszl/202109/t20210918_2320918.html (in Chinese)
[463] https://www.spp.gov.cn/spp/xwfbh/wsfbt/202104/t20210407_514984.shtml#1 (in Chinese)

banks and has led the country to rank second worldwide in banking fraud, as reported by Muggah and Nathan (2015). Although cybercrime in Brazil is significant, the country experiences "traditional" violent crime, which clearly dominates the attention, absorbs most of the resources and leaves few law enforcement agents to deal with cybercrime issues (Kshetir and DeFranco, 2020). To make matters worse, since the cybercrimes are localised, they have not attracted the attention (and have not triggered the detection capabilities) of the international community. As a result, local banks, in a cat-and-mouse game with cybercriminals, have developed strong security measures and probably are world leaders in defending against cybercrime (Lusthaus, 2018b).

Brazil is also a major victim of cybercrime. A survey pointed out that in the first semester of 2021, the country exceeded the volume of attacks of the whole previous year. In particular, 9.1 million ransomware attacks makes the country the fifth biggest cybercrime target globally.[464] In the private sector, fewer than a third of Brazilian organisations have a cybersecurity team.[465] Moreover, although cyber threats have amplified since the outbreak of the COVID-19 pandemic, organisations in Brazil have not increased their investments in cyber security and most of them invest 10 per cent or less of their budget for information security.[466] For instance, in November 2020, the Brazilian aerospace firm Embraer suffered from a cyberattack that made its systems unavailable.[467] Allegedly, it was a ransomware attack.[468] More recently, in June 2021, Brazil medical firm Fleury was hit by the REvil ransomware.[469] The cybercriminals behind this attack claim to have acquired sensitive medical and financial data.[470] In the public sector, cyberattacks have also become more common. In November 2020, cybercriminals launched a major cyberattack against the Brazilian Superior Court of Justice (STJ). As a result, the court suspended its operation for over two weeks as its information systems and virtual environment became unavailable after the attack.[471] In August 2021, the Brazilian Ministry of Economy announced that the National Treasury was target of a ransomware attack.[472]

At the national level, Brazil has taken significant steps to combat cybercrime. In 2018, the government published its National Information Security Policy[473] and then, in 2020, the government adopted its National Cybersecurity Strategy which includes the key objectives of

464 https://epocanegocios.globo.com./Tecnologia/noticia/2021/09/brasil-e-o-5-maior-alvo-de-crimes-ciberneticos.html (in Portuguese)
465 https://www.zdnet.com/article/most-brazilian-companies-lack-cybersecurity-teams
466 https://www.zdnet.com/article/brazilian-firms-fail-to-increase-security-spend-through-covid-19
467 https://thehack.com.br/embraer-tem-dados-vazados-apos-infeccao-pelo-mesmo-ransomware-que-atingiu-o-stj/ (in Portuguese)
468 https://www.infosecurity-magazine.com/news/aerospace-giant-embraer-hit
469 https://www.infomoney.com.br/mercados/fleury-e-o-mais-recente-episodo-de-ransomware-veja-como-os-ataques-ciberneticos-tem-afetado-os-mercados/ (in Portuguese)
470 https://www.bleepingcomputer.com/news/security/healthcare-giant-grupo-fleury-hit-by-revil-ransomware-attack
471 https://olhardigital.com.br/2020/11/05/seguranca/invasao-ao-stj-sequestrou-processos-e-backups-em-um-dos-piores-ciberataques-ja-vistos/ (in Portuguese)
472 https://www.gov.br/tesouronacional/pt-br/noticias/nota-do-ministerio-da-economia (in Portuguese)
473 http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm (in Portuguese)

increasing the country's digital reliability and resilience to cyber threats.[474] Furthermore, a cyberattack response network, the Federal Cyber Incident Management Network, was created in order to protect against cyber threats and improve the security of the federal public administration.[475] In this network, public and mixed capital companies will also participate voluntarily to strengthen more the role of the unit to mitigate future cyber threats.[476]

5.22.5 India

India has a large percentage of cybercrime victims. Statista reports that as many as 80 per cent of Internet users in India have reported that they have experienced cybercrime. The nature of cybercrimes ranges from petty online frauds to lottery scams, sexual harassment and child sexual abuse material (previously termed 'child pornography').[477] In particular, recent data from the National Crime Records Bureau (NCRB), an Indian government agency responsible for collecting and analysing crime data, show that cybercrime cases that involve children have increased by more than 400% in 2020 (i.e., the year the global pandemic was in full swing).[478]

However, the most targeted sector is banking and finance.[479] Reported cybercrime cases range to around 50,000 per year, and increase very rapidly. Most cases include online banking fraud, credit/debit card and ATM scams. NCRB also investigates the motives of people resorted to cybercrime. In addition to the obvious financial benefit of a cybercrime, people have resorted to it for other reasons such as sexual gratification, extortion, causing disrepute and personal revenge.[480] From a location perspective, the Indian states of Karnataka, Uttar Pradesh and Telangana prevail in financial fraud cases while the state of Maharashtra had the most cybercrime cases of sexual exploitation.[481]

Although India seems to be a major victim of cybercrime, it is not a powerhouse in producing cybercriminals or organised cybercrime. Indian cybercriminals are still at low-to-intermediate skill levels while cybercrime in India does not currently appear to be organised by larger criminal syndicates or have political and bureaucratic links (Mahadevan, 2020). Instead, it is developing in an environment of high unemployment, civil anonymity and weak police surveillance (e.g., a 2019 survey in 22 provinces of India found that one third of Indian police departments did not have a working computer) (Mahadevan, 2020). For these reasons, we can assume that in major cases of cybercrime in South Asia and India the main actors may come

474 https://www.zdnet.com/article/brazil-launches-cybersecurity-strategy

475 https://www.gov.br/casacivil/pt-br/assuntos/noticias/2021/julho/decreto-institui-a-rede-federal-de-gestao-de-incidentes-ciberneticos (in Portuguese)

476 https://www.zdnet.com/article/brazil-creates-cyberattack-response-network

477 https://www.statista.com/statistics /194133/cybercrime-rate-in-selected-countries

478 https://www.amarujala.com/india-news/cyber-crime-cases-against-children-increased-by-more-than-400-percent-in-the-year-2020-latest-news-update (in Hindi)

479 https://www.statista.com/topics/5054/cyber-crime-in-india/#dossierKeyfigures

480 https://www.amarujala.com/india-news/new-trend-of-cyber-crime-from-personal-rivalry-to-exploitations (in Hindi)

481 https://theleaderhindi.com/cyber-thugs-spreading-in-digital-india-broken-records-of-cyber-crime-in-covid-30755-2/ (in Hindi)

from foreign powers and are not necessarily local cyber criminals. Some major cybercrime cases are the following:

- In 2016, cybercriminals attacked the Bangladesh Bank and managed to steal US $81 million (after initially attempting to steal almost $1 billion US)[482]. Security researchers found evidence that the theft was committed by criminals backed by the government of North Korea.[483]
- In 2017, a cyber-attack occurred in the Union Bank of India. The attack was initiated when an employee accidentally opened a malicious email attachment. The attachment contained malware that allowed cybercriminals to gain access into the bank's system, steal SWIFT access codes and transfer $170 million to a Union Bank account at Citigroup Inc in New York.[484]
- In 2018, a massive data breach exposed more than one billion records of personal information from the Unique Identification Authority of India (UIDAI) Aadhaar software. UIDAI announced that 210 Indian government websites were hacked and the Aadhaar details of people leaked online.[485] Anonymous sellers were selling Aadhaar information for Rs. 500 over WhatsApp.[486]
- In 2018, several cloned debit cards of Cosmos Bank were used for thousands of ATM transactions, totalling to Rs. 94.42 crore[487] (= about €9.5 million), from India and 28 other countries in a period of seven hours.[488]
- In 2018, cybercriminals targeted Canara Bank ATM servers and exposd the card details of more than 300 users. Cybercriminals gained access to the data by using skimming devices and managed to steal Rs. 20 lakh[489] (= about €200,000) from various bank accounts.[490]

As of 2018, India has the second largest newspaper market in the world, with daily newspapers reporting a combined circulation of more than 240 million copies.[491] Most of these newspapers have an online presence and it seems that they generally make reference to cybercrime. The Dainik Bhaskar newspaper is ranked fourth in the world and first in India by circulation.[492] The

[482] https://www.wired.com/2016/05/insane-81m-bangladesh-bank-heist-heres-know
[483] https://www.nytimes.com/2017/03/22/business/dealbook/north-korea-said-to-be-target-of-inquiry-over-81-million-cyberheist.html
[484] https://www.firstpost.com/tech/news-analysis/recent-cyber-attack-on-union-bank-in-india-was-similar-to-the-hack-attack-in-bangladesh-cyber-heist-3700825.html
[485] https://www.firstpost.com/tech/news-analysis/uidai-aadhaar-software-hacked-using-a-patch-which-disabled-critical-security-report-5159521.html
[486] https://www.zee5.com/zee5news/unlock-the-haunted-app-five-real-life-cyber-crime-cases-in-india-that-shook-the-world-66614-2 (in Hindi)
[487] A crore is equal to ten million in the Indian numbering system
[488] https://indianexpress.com/article/cities/pune/cosmos-bank-malware-attack-interpol-issues-red-corner-notice-against-prime-suspect-traced-in-foreign-country-6574097
[489] A lakh is equal to one hundred thousand in the Indian numbering system
[490] https://timesofindia.indiatimes.com/city/kolkata/golpark-atm-fraud-robs-over-50-people-of-rs-20-lakh/articleshow/65220319.cms
[491] https://en.wikipedia.org/wiki/List_of_newspapers_in_India
[492] http://www.auditbureau.org/files/JD%202019%20Highest%20Circulated%20(across%20languages).pdf

newspaper published an article about the incidents of cybercrime taking place in the country and their increase due to the COVID-19 pandemic.[493] It has also published articles to inform citizen on how to report a cybercrime either online[494] or at various police stations.[495] Aaj Tak, a Hindi-language news channel, has a special section dedicated to cybecrime.[496] Some of its articles make reference to the recent case of the Bulli Bai application, a malignant application which was created with purpose to harass and intimidate Muslim women. Technically, it is a piece of code hosted on GitHub, similar to software used in the Sulli Deals case in 2021[497], showing photos of prominent Muslim journalists and activists along with "prices" in order to present them as in a virtual auction. Police have already arrested five people for creating the Bulli Bai app.[498] Similarly to Aaj Tak, many online channels provide news about cybercrime and cyber frauds (e.g., livehindustan.com[499], zeenews.india.com[500], indiatv.in[501], amarujala.com[502], etc.).

AVERAGE AGE OF CYBERCRIMINALS: 32 YEARS OLD
Cambridge Computer Crime Database

5.23 The age dimension of cybercrime

5.23.1 Perpetrators

Previous studies have suggested that offenders vary in age (Lusthaus (2018b)). Demographic studies of traditional crime (i.e. non cybercrime) suggest that the age distribution is skewed towards people in their teens and their twenties. Cybercrime is no exception. Although there does not exist a central database of all cybercrimes which can be used to find the age distribution of perpetrators, Lusthaus (2018b) reports that the average age is between 25 and 30 with a range varying from teenagers to senior citizens. In the same spirit, Hutchings and Collier (2019) studied the data contained in the Cambridge Computer Crime Database (CCCD) and found the records for which the age of the offender (at the time of the arrest or at the time of the most recent court hearing) was recorded. They report that ages vary from 14 to 69 years old with an average of 32.1 years. This obviously does not mean that these offenders were not involved in

493 https://www.bhaskar.com/business/news/317-lakhs-cyber-crimes-in-india-in-just-18-months-says-government-128305693.html (in Hindi)
494 https://www.bhaskar.com/local/bihar/patna/news/know-the-rights-of-yours-from-expert-if-you-face-cyber-crime-ever-129225718.html?ref=inbound_More_News (in Hindi)
495 https://www.bhaskar.com/local/rajasthan/bikaner/news/police-set-up-cyber-crime-response-cell-information-can-be-given-on-the-number-129338225.html (in Hindi)
496 https://www.aajtak.in/crime/cyber-crime (in Hindi)
497 https://www.aajtak.in/crime/cyber-crime/story/delhi-police-registers-fir-in-sulli-deals-case-investigation-begins-1287159-2021-07-08 (in Hindi)
498 https://www.aajtak.in/crime/cyber-crime/story/bullibai-app-case-mumbai-court-sends-accuses-arrested-from-odisha-to-police-custody-ntc-1397679-2022-01-23 (in Hindi)
499 https://www.livehindustan.com/crime/cyber-crime/news (in Hindi)
500 https://zeenews.india.com/hindi (in Hindi)
501 https://www.indiatv.in/topic/cyber-crime (in Hindi)
502 https://www.amarujala.com/tags/cyber-fraud?page=1 (in Hindi)

cybercrime when they were younger. However, the data available suggest that these cybercriminals were engaged in cybercrime well beyond their teens – in their twenties and thirties. At this point we must say that the actual age of the perpetrators depends heavily on the type of cybercrime. For example, the previously mentioned average age of 32.1 years old (for the Cambridge Computer Crime Database) was for cybercriminals engaging in cyber-dependent cybercrime including malware, data breaches, fraud, DoS attacks, etc. Hadzhidimova and Payne (2019) focus on international cyberoffenders and report that the average age is 34.79 with a range between 19 and 73. Hadzhidimova and Payne (ibid.) focus on cybercriminals who engage in cyber-dependent crime. Their data are from the U.S. Department of Justice press releases between January 2009 and December 2017.
Perpetrators engaged in other types of cybercrime may be older. For example, Lee et al. (2012) suggest that the average age of CSAM perpetrators was 41. Buschman et al. (2021) reached exactly the same average age (41) of CSAM perpetrators with a range between 26 and 64.

5.23.2 Victims

The victims of sex-related crimes seem to be very young. For example, the victims of CSAM (by definition) are minors. Wolak et al. (2012) reports that the victims of sextortion are also young – most of the responders in their survey report that sextortion started when they were 17 or younger. Van Heugten et al. (2021) report that victims of sextortion from Nigeria are mostly females between 13 and 35 years old. For other types of cybercrime such as Fraud and Theft it seems that the ages of the victims are larger and the range much wider. For example, Schreuders (2018) reports that victims of Fraud and Theft are both males and females aged 16 to 45. Actually, Schreuders (ibid.) reports that the likelihood of becoming victim to this type of cybercrime increases with age.

6 Cybercrime-as-a-Service (CaaS)

6.1 Cryptocurrency laundering and tumbling 201
6.2 Bulletproof hosting 202
6.3 Tutorials, training and consulting 204
6.4 Hacking-as-a-Service 204
6.5 Coding/Programming-as-a-Service 205
6.6 Crypting - obfuscation 205
6.7 Distributed denial-of-service (DDoS) attacks/Reflection attacks (DRDoS) 206
6.8 SMS flooding and spamming 209
6.9 Escrow/Garant/Treuhand 209
6.10 Fast-Fluxing - a moving target 210
6.11 Mules 212
6.12 Proxy servers 213
6.13 VPN Servers 214
6.14 Email spamming and phishing 214
6.15 Crimeware - Ransomware-as-a-Service 215
6.15.1 Pay-per-install (PPI) 216
6.15.2 Affiliate programme 217
6.16 Data-as-a-Service (DaaS) 217
6.16.1 Credit card credentials 218
6.16.2 Carding 218
6.16.3 Bank account credentials - stolen accounts 218
6.16.4 Non-banking account credentials - stolen accounts 219
6.16.5 Phone number databases 219
6.16.6 Fake documents - identity theft 219
6.16.7 PII querying 220
6.17 Serial keys - pirated software 220
6.18 Social boosters - friends and "likes" for purchase 221
6.19 Web traffic - visitors 221
6.20 Cybercriminal business, marketing and messaging 222
6.21 Underground forum access 223

In recent years, cybercrime has adopted practices similar to those of legitimate businesses.[503,504] 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.

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

[503] https://www.welivesecurity.com/2016/12/08/cybercrime-business-model-value-chain/
[504] https://www.iotworldtoday.com/2017/06/14/8-strategies-transition-product-service-business-model/

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).

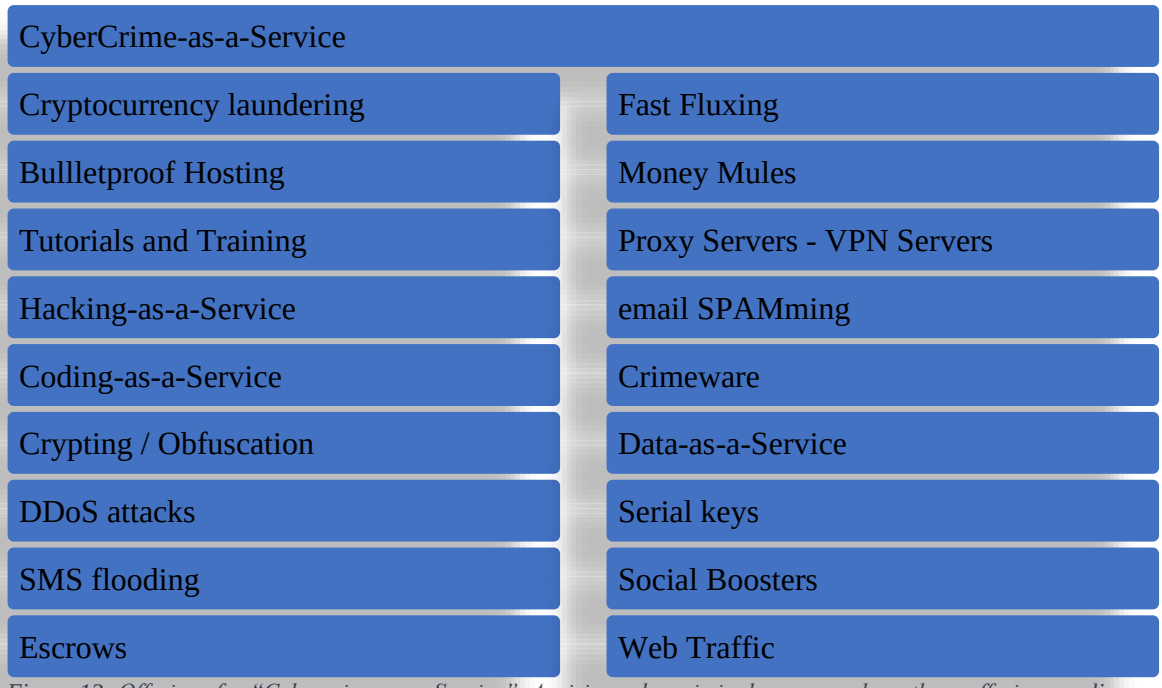


Figure 13: Offerings for "Cybercrime-as-a-Service". Aspiring cybercriminals may purchase these offerings on-line and thus ease their way into conducting cybercriminal activities.

6.1 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**".

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.[505] 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 $100 million US in bitcoins from a site for drug dealers called Sheep Marketplace and tried to hide the money by using various tumblers.[506] 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.[507] 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 US at the time of the transactions.[508] During 2017, about $266 million US was laundered through cryptocurrencies, while this amount was tripled ($761 million US) in the first half of 2018.[509]

[505] 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.
[506]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
[507] https://thenextweb.com/news/chinese-bitcoin-exchange-bter-will-pay-back-users-after-losing-1-75-million-in-cyberattack
[508] https://www.justice.gov/opa/pr/individual-arrested-and-charged-operating-notorious-darknet-cryptocurrency-mixer
[509] https://www.americanbanker.com/news/crypto-money-laundering-rose-3x-in-first-half-2018-report

Cybercriminals also utilise 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).[510] In 2020, just in the Bitcoin ecosystem, $3.5 billion US 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.[511]

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.[512] Bitconnect token was among the top 20 cryptocurrencies in the world in terms of market value in early 2018.[513] Subsequently, the former head of BitConnect was arrested in India for promoting another cryptocurrency called "Regal coin", promising very high returns (up to 45% per month); this also turned out to be a scam.[514]

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.[515] 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.[516,517]

6.2 Bulletproof hosting

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

[510] https://cointelegraph.com/news/pwc-bitcoin-ransomware-hackers-laundered-money-via-wex-exchange
[511] https://ciphertrace.com/2020-year-end-cryptocurrency-crime-and-anti-money-laundering-report/
[512]https://www.independent.co.uk/life-style/gadgets-and-tech/news/bitcoin-scam-bitconnect-cryptocurrency-regal-coin-a8945291.html
[513] https://www.fool.com/investing/2017/07/20/the-20-largest-cryptocurrencies-by-market-cap.aspx
[514] https://quickpenguin.net/regalcoin-scam/
[515] https://paybis.com/blog/what-is-kyc/
[516] https://shuftipro.com/blog/anti-money-laundering-compliance-for-crypto-exchanges-2021-update/
[517] https://www.forbes.com/sites/vishalmarria/2018/09/13/eu-5th-anti-money-laundering-directive-what-does-it-mean/

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 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.[518]

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.[519]

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.

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

6.3 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. 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.

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.[520]

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.

6.4 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,

[520] 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.

cybercriminals bypass password authentication using answers to "secret questions". Such questions include "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[521] or slightly higher prices[522] 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.[523] At this point, we should also add that in some of the cases such advertisements are just scams that steal the money from clients.

6.5 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).

6.6 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 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

[521] https://socialhacking.pro/
[522] https://www.instabitnetwork.com/pricing/
[523] https://hireahacker.ninja/

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.[524] The popular RAZ crypter can be found for rent for $25 US for one month or $40 US for three months.[525]

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

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

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

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.[526] 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.[527] 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.[528]

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).

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.

[526] 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.
[527] https://www.privacyaffairs.com/dark-web-price-index-2021/#9
[528] https://www.welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices/

- 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.[529] 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.[530]

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 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.[531]

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

[529] https://www.networkworld.com/article/2164810/ddos-attack-against-spamhaus-was-reportedly-the-largest-in-history.html
[530] https://www.rfc-editor.org/rfc/rfc2827.txt
[531] https://blog.cloudflare.com/no-scrubs-architecture-unmetered-mitigation/

is with anycast routing.[381,532] This kind of mitigation for the largest attacks requires enormous network capacity, which only few organisations have.[533]

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.[534]

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.[535]

6.8 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).

6.9 Escrow/Garant/Treuhand

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

[532] https://www.cloudflare.com/learning/cdn/glossary/anycast-network/
[533] https://blog.cloudflare.com/reflections-on-reflections/
[534] https://www.cloudflare.com/learning/ddos/glossary/ddos-blackhole-routing/
[535] https://blog.nexusguard.com/threat-report/ddos-threat-report-2019-q1

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,[536] typically 1-15%[537] 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[538].

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. 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.

6.10 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

[536] https://www.digitalshadows.com/blog-and-research/escrow-systems-on-cybercriminal-forums/
[537] https://www.deepwebsiteslinks.com/bitcoins-escrow-services/
[538] https://www.digitalshadows.com/blog-and-research/escrow-systems-on-cybercriminal-forums/

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 (Wainwright & Cilluffo, 2017).[539] 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.[540] 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.[541]

[539] "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.
[540] https://krebsonsecurity.com/2016/05/carding-sites-turn-to-the-dark-cloud/
[541]https://www.proofpoint.com/us/threat-insight/post/sandiflux-another-fast-flux-infrastructure-used-malware-distribution-emerges

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

6.11 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.[542]

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.[543] 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.[544] Reportedly, these mules facilitated the transfer of more than US $3 million.

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.[545]

As the FBI states in its "Common scams and crime"[546] report, individuals advertise their services as a money mule (probably on the Dark Web), to include what actions they offer and at what prices.[547] Moreover, mule advertisements have also been observed in Japanese underground bulletin board systems (BBSs), where cybercriminals exchange various messages and job opportunities (Urano, 2015).

[542] https://www.rsa.com/en-us/blog/2016-04/money-mules-the-critical-cash-out-service-in-the-fraud-supply-chain
[543] https://www.europol.europa.eu/activities-services/public-awareness-and-prevention-guides/money-muling
[544] https://archives.fbi.gov/archives/newyork/press-releases/2010/nyfo093010.htm
[545] http://www0.cs.ucl.ac.uk/staff/G.Stringhini/papers/shipping-ccs2015.pdf
[546] https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/money-mules
[547] https://www.commercial-bank.com/userfiles/filemanager/61794706gop6pznpm7p2/

6.12 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.

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 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.[548] 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).

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

6.13 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.[549]

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, 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.[550]

6.14 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

[549]https://www.europol.europa.eu/newsroom/news/cybercriminals%E2%80%99-favourite-vpn-taken-down-in-global-action
[550]https://www.kroll.com/en/insights/publications/cyber/monitor/vpn-vulnerabilities-rising-data-exposure-ransomware

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.[551] 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 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).[552]

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).

6.15 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

[551] https://www.trendmicro.com/vinfo/mx/security/news/cybercrime-and-digital-threats/emotet-uses-coronavirus-scare-in-latest-campaign-targets-japan
[552] https://www.privacyaffairs.com/dark-web-price-index-2021/#8

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).

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.[553]

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 customised to attack specific targets.[554] 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.[555]

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.[556]

6.15.1 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

[553] https://www.cyberscoop.com/mirai-botnet-for-sale-ddos-dark-web/
[554] https://ransomware.fandom.com/wiki/Ranion_Ransomware
[555] https://www.welivesecurity.com/2019/01/31/cybercrime-black-markets-dark-web-services-and-prices/
[556] https://isc.sans.edu/forums/diary/Phishing+kits+as+far+as+the+eye+can+see/26660/

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).

6.15.2 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 more. Ryuk affiliates were reported to have collected at least $34 million from a single victim in 2020.[557]

6.16 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[558] 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).

[557] https://www.bleepingcomputer.com/news/security/dozens-of-ransomware-gangs-partner-with-hackers-to-extort-victims/
[558] https://en.wikipedia.org/wiki/Credit_card_fraud#Skimming

6.16.1 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.[559]

6.16.2 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 business. As per Gemini advisory, such payment/gift cards typically sell at 10% of their value on the underground market.[560]

6.16.3 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,[561] 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

[559] https://www.privacyaffairs.com/dark-web-price-index-2021/#2
[560] https://geminiadvisory.io/gift-card-shop-breached/
[561] https://www.privacyaffairs.com/dark-web-price-index-2021/#5

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.

6.16.4 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 cheap 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.[562]

6.16.5 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).

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.[563]

6.16.6 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

[562] https://www.privacyaffairs.com/dark-web-price-index-2021/#5
[563] https://www.troyhunt.com/the-facebook-phone-numbers-are-now-searchable-in-have-i-been-pwned/

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.[564]

6.16.7 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 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.[565]

6.17 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

[564] https://www.privacyaffairs.com/dark-web-price-index-2021/#7
[565] https://www.itproportal.com/features/pricing-of-goods-and-services-on-the-deep-dark-web/

sources of such keys are in most cases illegal and police have been issuing charges for copyright infringement and money laundering.[566]

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).

6.18 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.

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.[567]

6.19 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 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).

[566] https://tarnkappe.info/windows-10-lizenzkeys-staatsanwaltschaften-verschicken-vorladungen/
[567] https://www.privacyaffairs.com/dark-web-price-index-2021/#5

6.20 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).

6.21 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.[568]

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.

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

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

7 Connections between cyber and traditional crime

As crime has increasingly moved online, the borders between cybercrime and crime in the physical world have been blurred. Europol (2021) acknowledges technology as a key feature of serious and organised crime in 2021. For instance, criminals use cryptocurrencies and encrypted communications among themselves, and social media to reach large audiences. Furthermore, criminals engage in online trade (both surface and dark web) to access expertise and tools that enable criminal activities, and to market both cybercrime services, such as hacking and malware, and traditional crime services, such as perpetrating violence on behalf of a criminal client. New hybrid forms of crime appear, and cyber activities are used to enable traditional crime. The Europol IOCTA (2020) report states that, as cybercrime evolves, the cyber-element of cybercrime infiltrates nearly every area of criminal activity.

There is a lack of systematic studies and statistics relating to the connections between cyber and traditional crime, and the hybrid forms of crime that involve aspects of both. This is much affected by definitional issues of cybercrime and challenges in collecting data. For instance, Caneppele and Aebi (2019), while discussing the debate around the reasons behind the drop in traditional crime and proposing a connection to the increase in cybercrime, note that the official crime statistics do not present a comprehensive picture of the situation. Definitional issues, as well as issues in the statistical counting rules related to cybercrime, raise obstacles for this type of research of the cybercrime world.

Cybercrime trends identified by the German Federal Criminal Police Office (2021, p. 4) cast some light on the conceptual nuts and bolts of the similarities and differences between cybercrime and traditional crime. Broadly speaking, numerous cybercrime trends aim at acquiring information (i.e. identity theft), causing damage (i.e. certain forms of malware—among other things, in the sense of undermining the functionality of a third party's system using ransomware or DDoS), selling fake products or spreading disinformation. From a highly abstract perspective, the overall objectives that inform the cybercrime trends are not new. Identity theft to engage in fraudulent business interactions existed before the Internet age. The same is true of selling fake products to make money and spearheading disinformation campaigns to sow division. The first is as old as merchandise itself and the second has been a long-standing component of all sorts of ideological confrontations; the Cold War between East and West is a case in point. The disruption of a third party's activities is not new either—although, to be fair, it was way more challenging prior to the Internet age. Even ransom as such is far from new, although the encryption of IT systems to force the other side to pay ransom is an entirely different criminal approach.

This observation leads us to a very important consideration, namely that the tools and techniques of modern cybercrime may differ so greatly from criminal activities that are driven by similar goals that cybercrime may constitute a form of crime in its own right. This is a particularly valid point in cases where the use of the cyber realm is required to commit certain criminal activities, such as encrypting the access to IT systems. As old as the attempts to steal someone else's identity, to cause damage, to sell fake products or to spread disinformation may be, many of the exact criminal activities could not be carried out without the use of new technology.

The insight that the use of the cyber realm is a prerequisite for many cybercrimes is at the heart of the distinction between cyber-dependent and cyber-enabled crimes. The former could not be

carried out without the use of IT systems, whereas the latter are only IT-supported (McGuire & Dowling 2013).

This distinction is well illustrated by Europol (2020), whose cybercrime report devotes a special section to cyber-dependent crime. Quite tellingly, the ransomware issue is particularly emphasised as the most urgent threat in the realm of criminal proceedings that could not be committed without the Internet. Malware and DDoS attacks are also mentioned as significant threats. Child sex exploitation and payment fraud, however, are not considered cyber-dependent crimes, as they could also be conducted without the use of IT systems.

This list of cyber-dependent crimes bridges the gap between the comparison of cybercrime and traditional crime and the key cybercrime threats as identified by the German Federal Criminal Police Office (2021). These threats are largely identical to Europol's threat assessment concerning the cyber-dependent crime realm, which corroborates the threat analysis of both players, but also highlights the importance of the Internet as a tool to commit the most essential and dangerous cybercrimes.

German law-enforcement agencies agree that many criminal activities could not be carried out in the absence of the new technology. In contrast with the aforementioned dichotomy, however, they distinguish between cybercrime in a narrow and cybercrime in a broader sense. The first set of criminal activities specifically targets the Internet, IT-relevant systems or their data, whereas the second is carried out through the use of IT (Federal Criminal Police Office 2021).

Admittedly, this distinction makes it somewhat challenging to draw conclusions about the similarities and differences of cybercrime and traditional crime. While cybercrimes in a narrow sense that target the Internet, IT-relevant systems or their data certainly aim at the cyber realm, and would require different targets if the latter did not exist, it is not clearly addressed what role IT-related tools play with respect to the nefarious activities as such. It takes an overview of the cybercrime activities that fall under the relevant definition to comprehend that such IT-related tools actually play quite a pivotal role. Among other things, cybercrimes in a narrow sense include computer fraud, spying on and retrieving digital data (Federal Criminal Police Office 2021).

Unlike cybercrime in a narrow sense, cybercrime in a broader sense casts a little more light on the similarities and differences of cybercrime and traditional crime in the sense that it clearly emphasises the use of IT to commit crimes. However, strictly speaking, the definition of cybercrime in a broader sense does not rule out that traditional forms of crime using non-IT tools might also be used to conduct the relevant crimes.

Hybrid forms of crime that comprise both cyber and traditional crime get little attention in cybercrime classifications. Caneppele and Aebi (2019) propose a classification that distinguishes between 1) traditional crime i.e., offline crime, 2) cybercrime, which takes place exclusively online and includes both cyber-enabled and cyber-dependent types of crime, and 3) hybrid crime, which combines both online and offline components. As mentioned above, there are definitional issues, as well as a lack of research and statistics related to hybrid forms of crime. However, multiple examples of this type of crime can be found in studies, LEA reports and media articles.

Next, some examples representing the variety in hybrid crime trends are described.

ATM attacks. Europol (2020) identifies logical attacks on ATMs and POS devices as a continuing threat that has increased across Europe. In particular, black-box attacks are common and used by organised criminal groups, which are often Russian-speaking and have connections to Eastern Europe. Black-box attacks require little technical knowledge besides the provision of the external device, which is connected to the cash dispenser, and instructions. These attacks can rapidly affect different geographic locations, as cybercriminals remotely send instructions for criminal networks to jackpot the ATMs. These attacks have also included new forms of *modus operandi*, even including a criminal group using malware to check the balance of an ATM before deciding to attack it.

Motor vehicle crime is an area of crime that is increasingly technical. Modern motor vehicles have many digital components that are vulnerable to cyberattacks, and most thieves rely on electronic compromise of the vehicle systems to overcome the improved vehicle security. Vehicles are often stolen by exploiting new technologies, such as relay attacks, to reprogram the vehicle and disable immobilisers, car alarms, and tracking systems alarms and tracking systems. (Europol 2021). Toolkits for these attacks are sold, among other places, in the dark web criminal marketplaces (Trend Micro 2019).

Cyber fraud is not new, but is still a rising form of property crime in Europe, and organised crime groups are incorporating cyber elements into their scams (Europol 2020). The types of widespread cyber fraud include card-not-present fraud, bank and credit account fraud and romance fraud. The role of the internet varies significantly in cyber fraud, but most cyber frauds can be labelled as cyber-enabled crime, meaning they are only IT-supported (Kemp et al., 2020). An example of this, observed by the Hellenic Police over the last two or three years, has been the rise in cyber financial crimes such as investment fraud schemes. In these schemes, the cyber elements include 1) the perpetrators having access to the victims' computers using remote access software, 2) the perpetrators contacting victims through social media profiles and emails, 3) the perpetrators giving victims access to online investment platforms, and 4) the fraudulent investment companies having online activity only.

Sextortion is another example of hybrid crime which is a growing business for criminals. Sextortion occurs when a perpetrator blackmails a victim with sensitive material, such as sexual images, that the perpetrator possesses or claims to possess. This material has often been obtained through “catfishing” (meaning that victims have been tricked into sending the sensitive material, typically on social media sites), by hacking the victim’s electronic devices or social media accounts, or remote webcam hacking, which might occur through email phishing schemes and malware. This can be even done on a mass-scale using botnets and botnet services (Carlton, 2020).

Of the abovementioned definitions, the classification of Caneppele and Aebi (2019) is the only one that considers the connections between cyber and traditional crime and the types of crime that include elements from both worlds. However, the few examples of hybrid crime described above draw a picture of a complex area of crime. The hybrid forms of crime represent an area that would need further research to understand the various ways in which cyber and traditional elements are connected in the criminal world.

8 Trends and correlations in the cybercrime landscape

8.1 SERVICE MODELS 229
8.2 MALWARE 230
8.2.1 Ransomware 230
8.2.2 PowerShell 234
8.3 COMMUNICATION METHODS 234
8.3.1 Tor 234
8.3.2 Email 236
8.3.3 Instant messaging 236
8.4 MONETISATION 237
8.4.1 Darknet/DarkWeb 238
8.4.2 Cryptocurrencies 239
8.5 SUMMARY 242

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.

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.

8.1 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.[569] In February 2021 Netskope estimated that 61% of malware is delivered via cloud, essentially hosted in various cloud services.[570] 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).[571]

Even instant message applications, such as discord, have been used to distribute malware.[572]

Nearly two thirds of ransomware incidents in 2020 were estimated to be related to a Ransomware-as-a-service (RAAS) platform.[573] RAAS has been available in the darknet since 2016[574] 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.

8.2 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.

8.2.1 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).

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

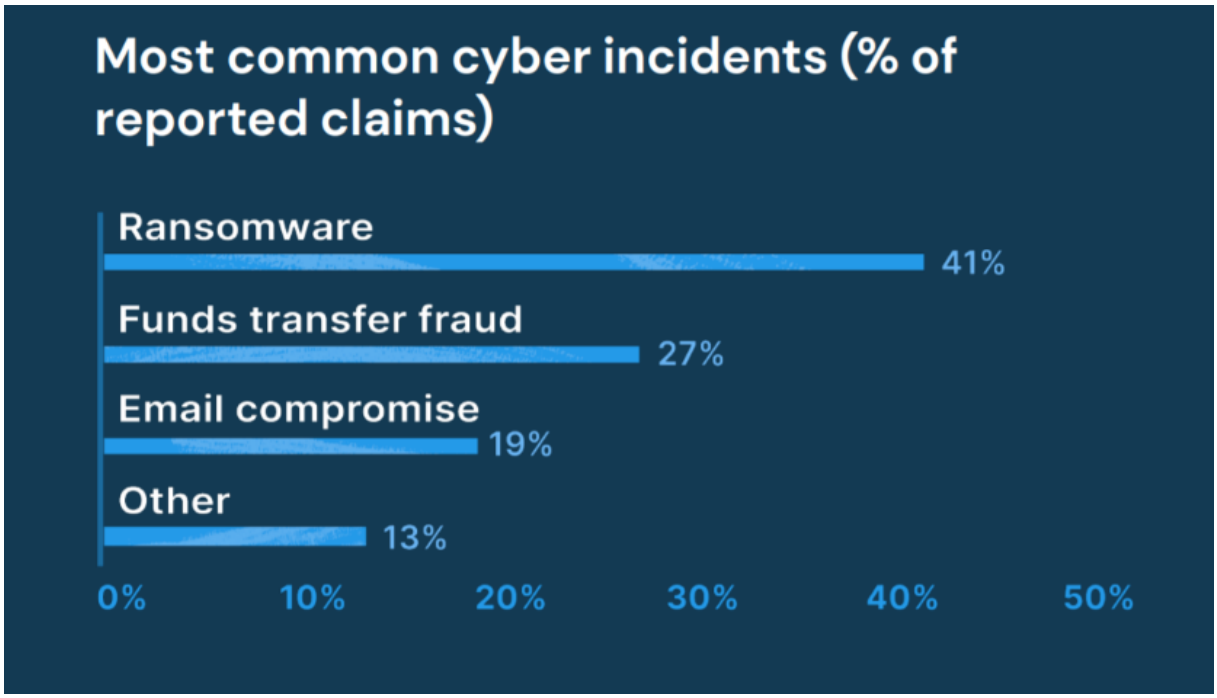


Figure 14:Insurance claims of cyber incidents (Coalition, 2020)

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).

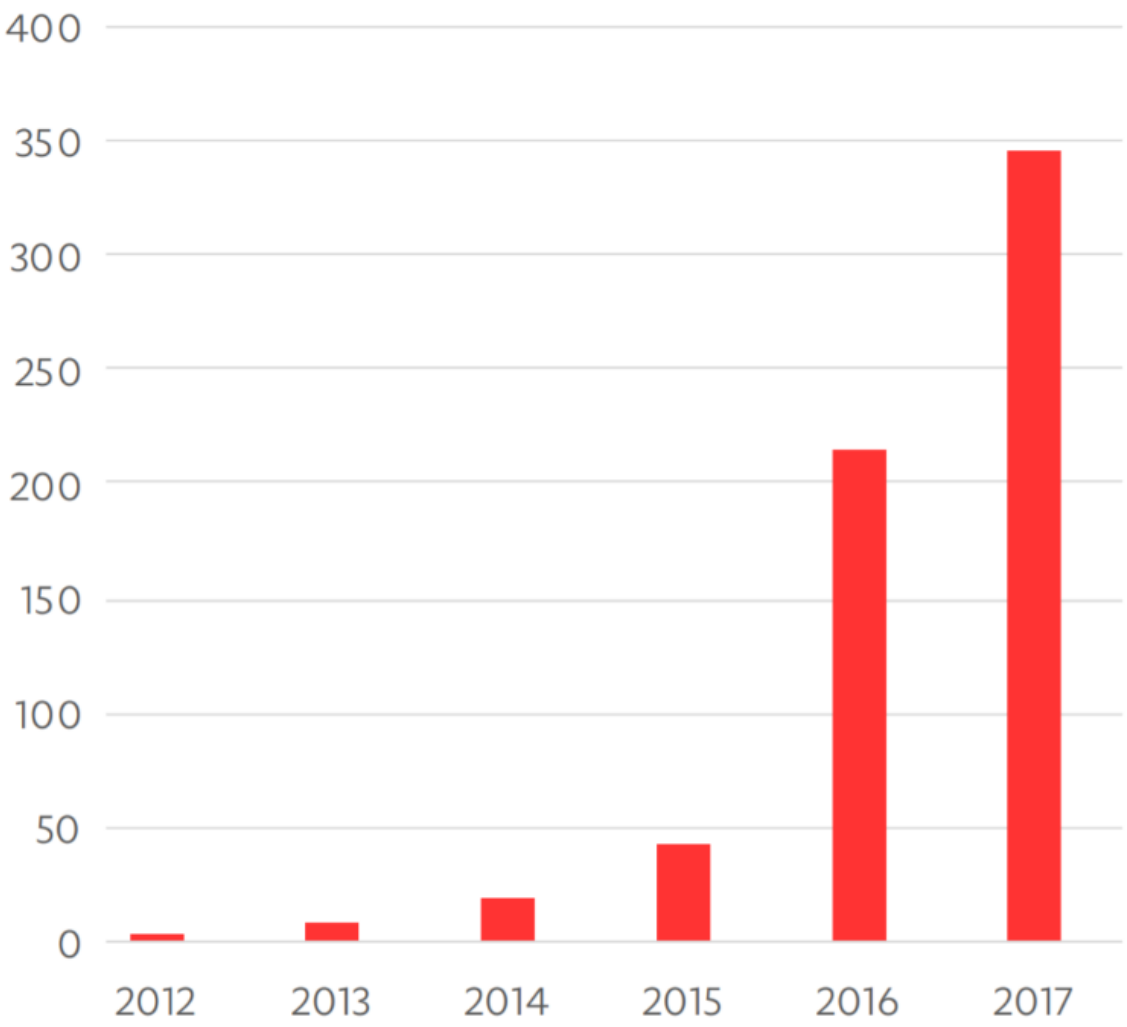


Figure 15: Number of unique ransomware families/variants (F-SECURE, 2018).

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.

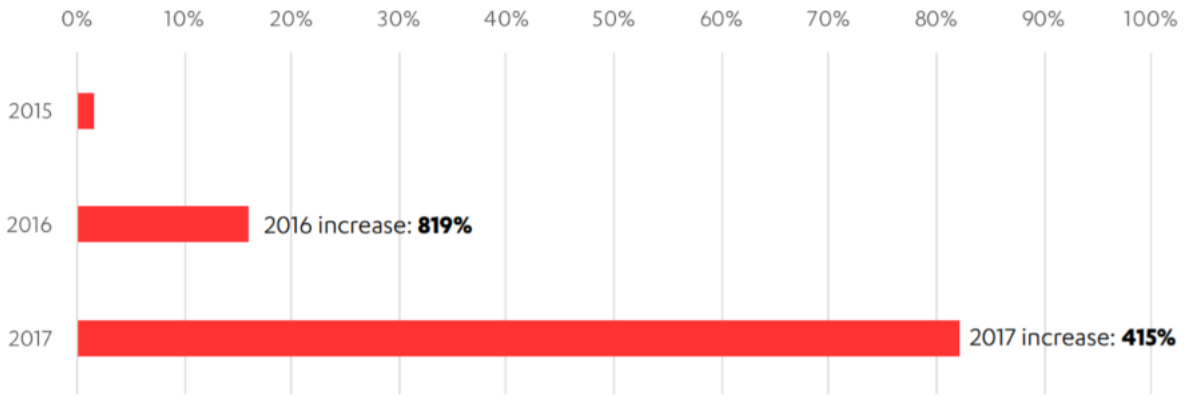


Figure 16: Number of detection reports per year based on percentage of total # of ransomware detections from 2015-2017 (F-SECURE, 2018)

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 observed in ransomware payments.[575] 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.

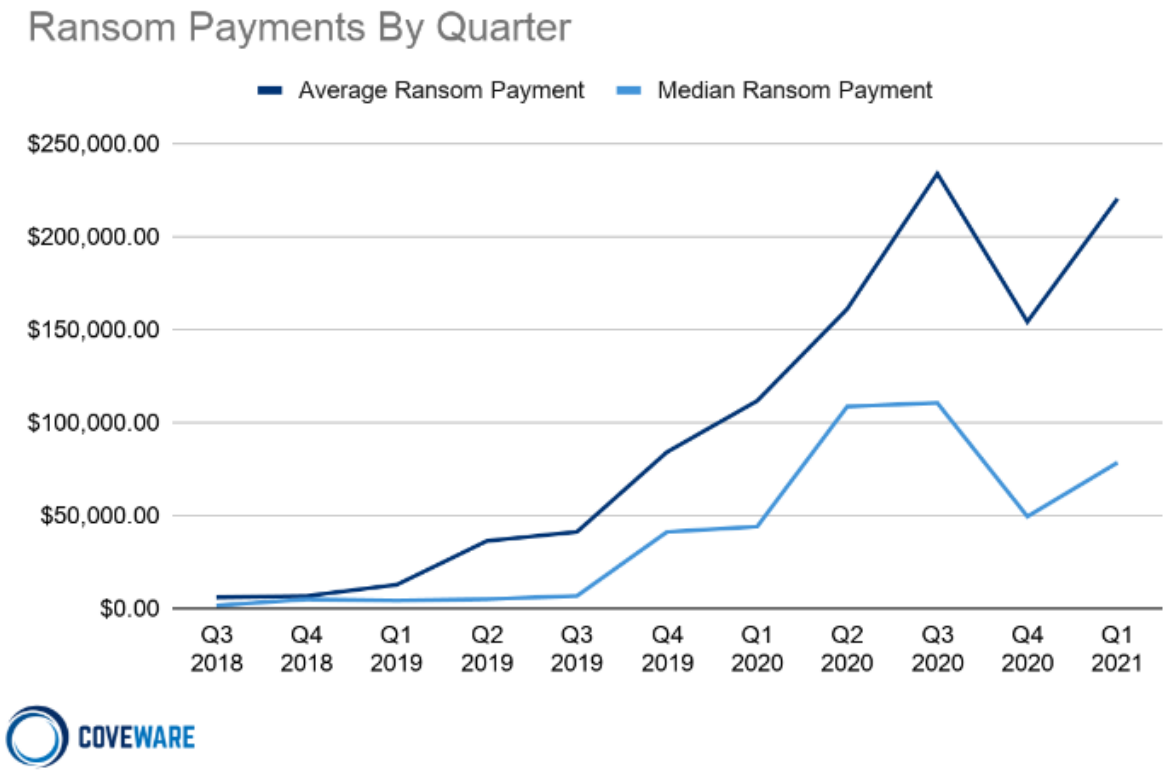


Figure 17: Amount of median & average ransom payments by quarter in USD (Coverware)[576]

[575]https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

[576]https://www.coveware.com/blog/ransomware-attack-vectors-shift-as-new-software-vulnerability-exploits-abound

8.2.2 PowerShell

PowerShell has seen significant use by cybercriminals in network breaches. In 2016, PowerShell was seen in more than a third of cyberattacks[577] 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.[578]

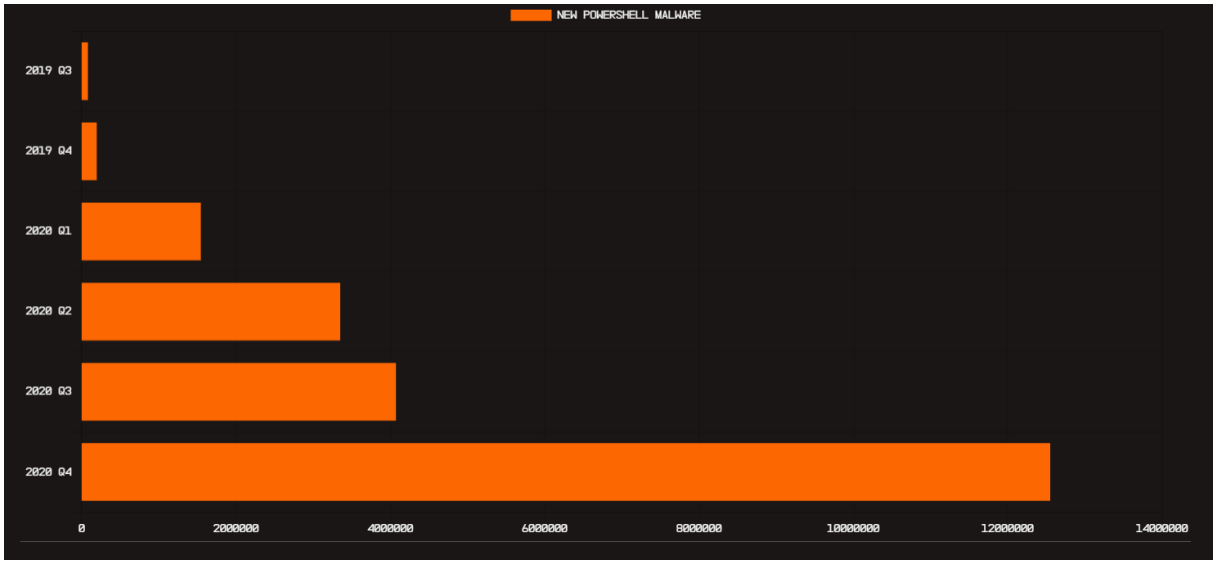


Figure 18: Numbers and growth of new Powershell malware in 2019 and 2021 as observed by McAfee

8.3 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.

8.3.1 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

[577] https://www.computerweekly.com/news/450281204/Windows-PowerShell-tied-to-more-than-a-third-of-cyber-attacks
[578] https://www.mcafee.com/enterprise/en-us/lp/threats-reports/apr-2021.html

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.

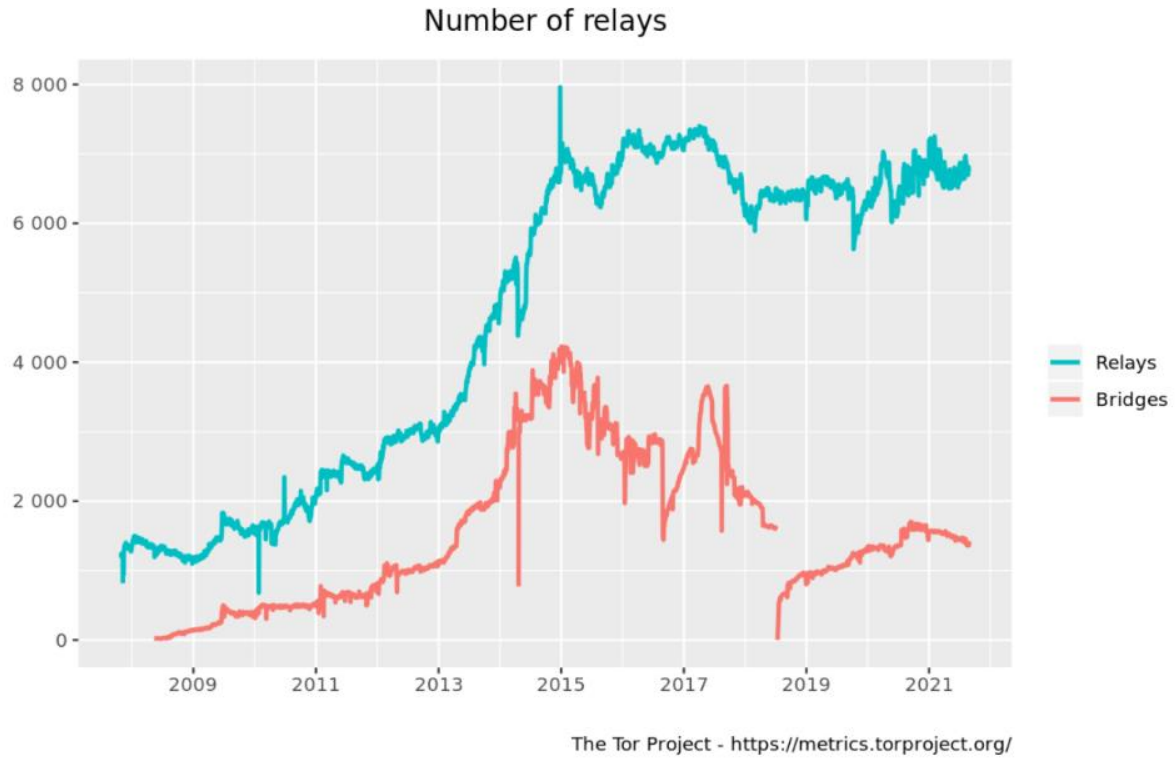
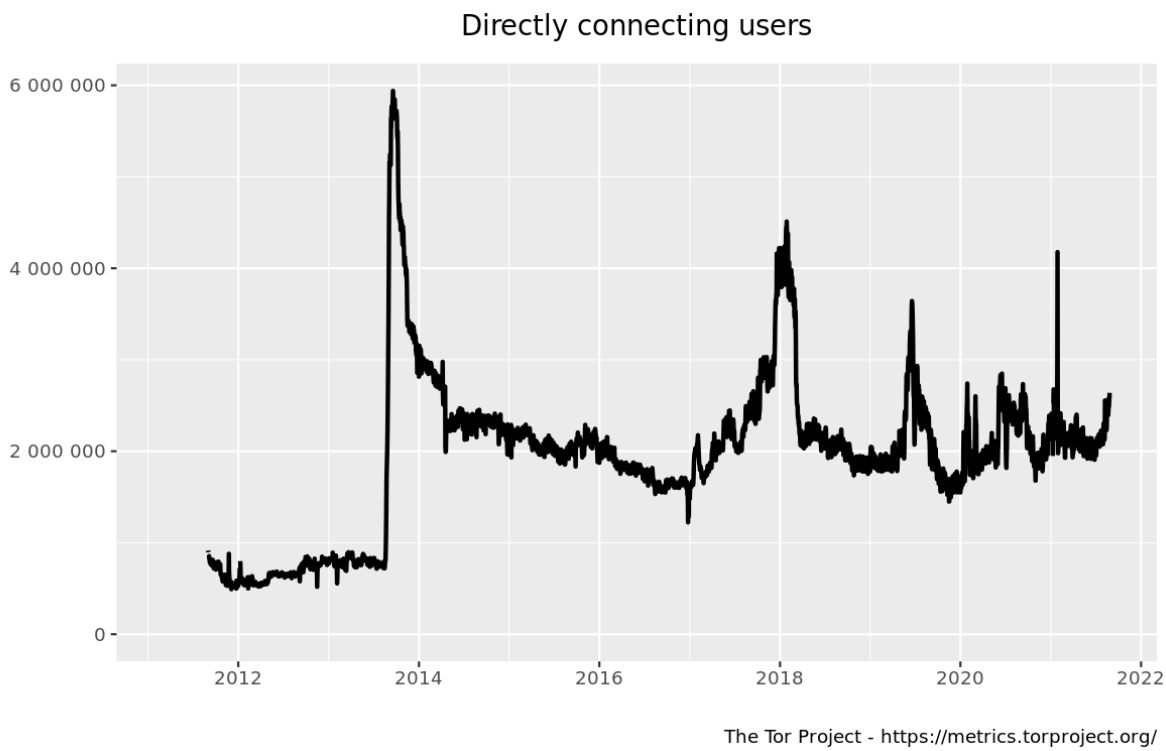


Figure 19: Number of tor relays & bridges since 2008

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,[579] 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.

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



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.

8.3.2 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.

8.3.3 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".[580]

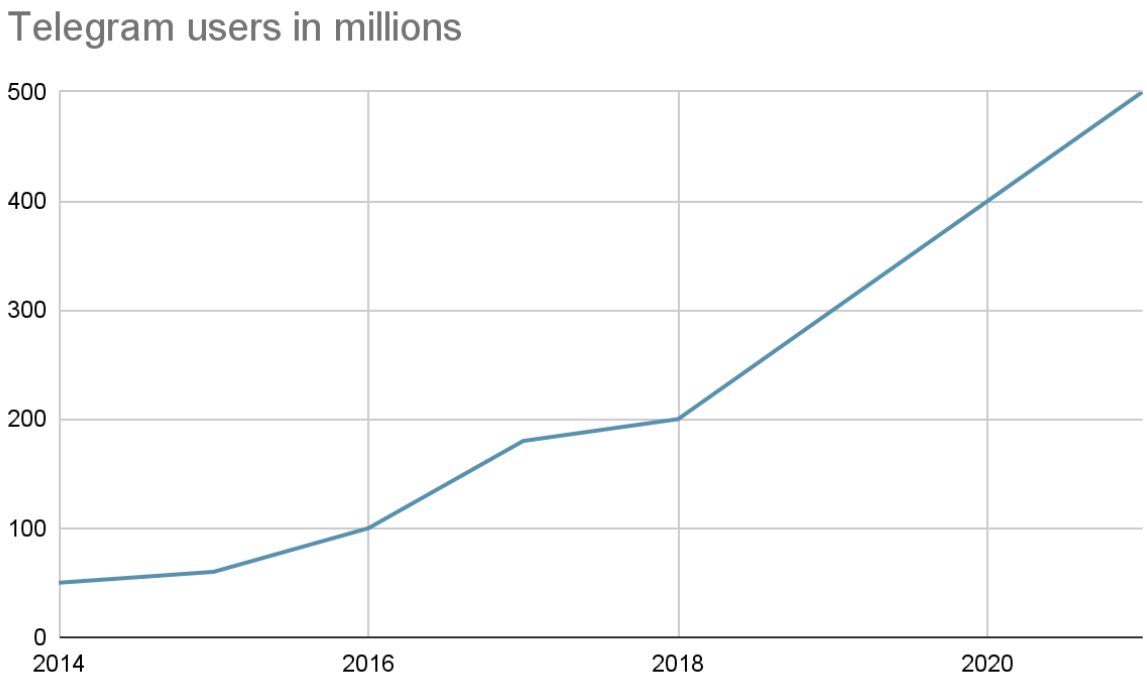


Figure 20: General Telegram popularity has been in a steady growth[581]

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.

8.4 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.

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

8.4.1 Darknet/DarkWeb

The darknet[582] 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%.[583]

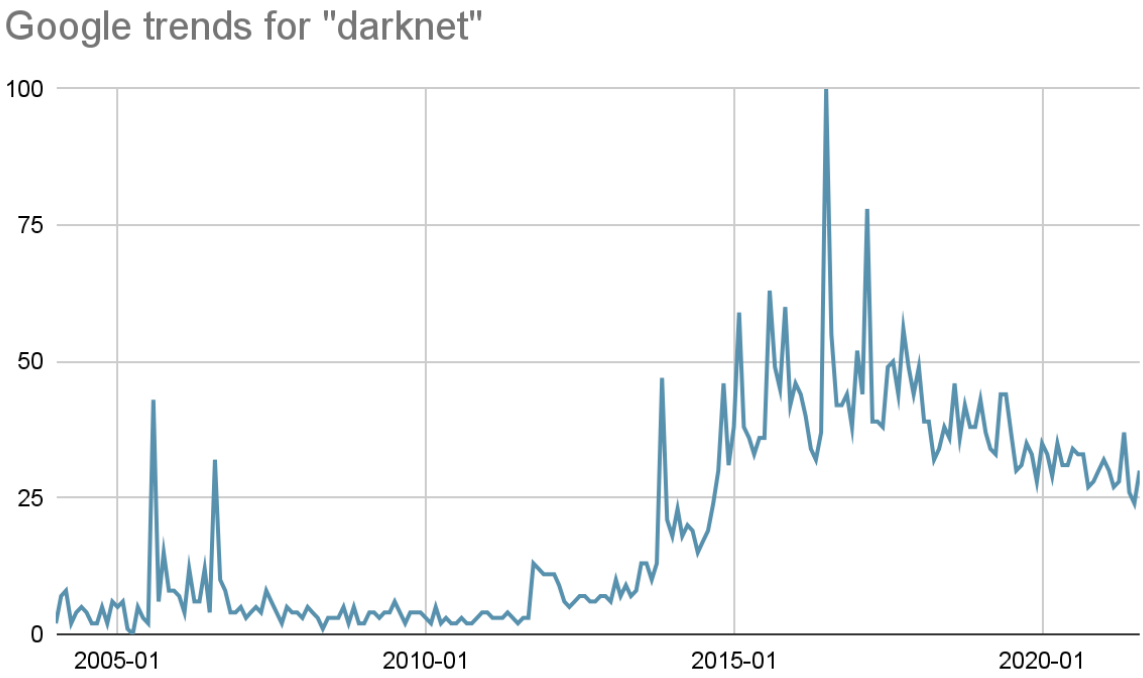
These offerings with impact potential include:

- 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.

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



8.4.2 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:

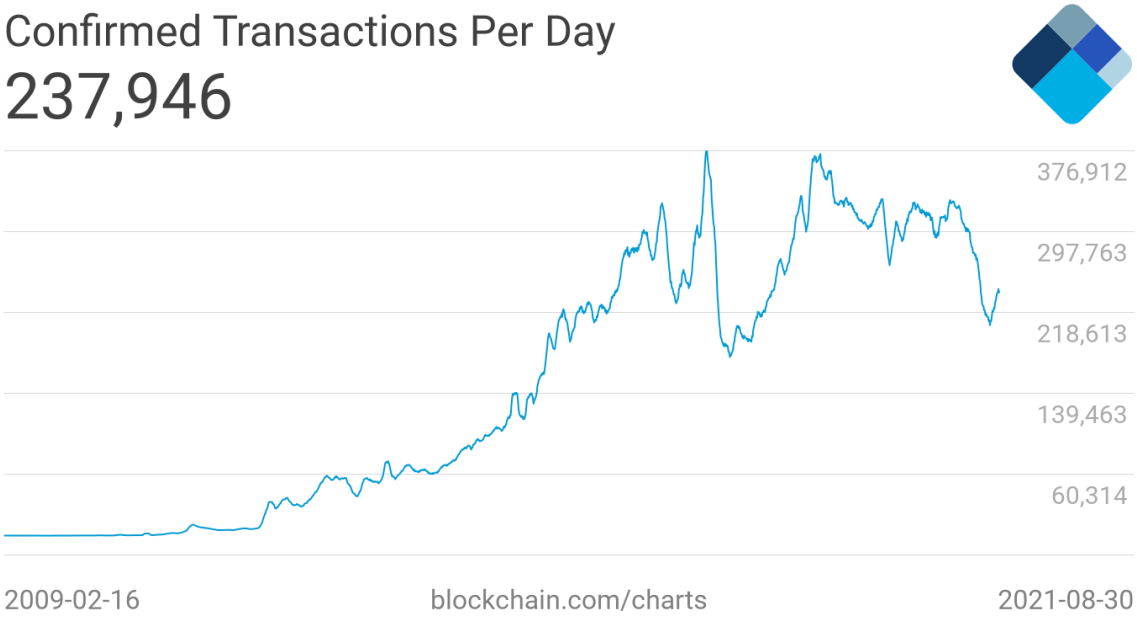


Figure 21: Bitcoin daily transactions 30 day average (Blockchain.com)[584]

In 2018, Europol estimated that about 5.5 Billion USD worth of money was laundered by criminals through cryptocurrencies.[585]

In 2019 the amount of cryptocurrency usage by criminals increased by over 300% and peaked at about 2% of total transfer value of cryptocurrencies.[586] While the number of criminal transfers are lower than 2019, the trend is upwards and is a significant amount of money (10 billion in 2020).

[584] https://www.blockchain.com/charts
[585]https://www.businessinsider.in/tech/criminals-in-europe-are-laundering-5-5-billion-of-illegal-cash-through-cryptocurrency-according-to-europol/articleshow/62888250.cms
[586] https://go.chainalysis.com/2021-Crypto-Crime-Report.html

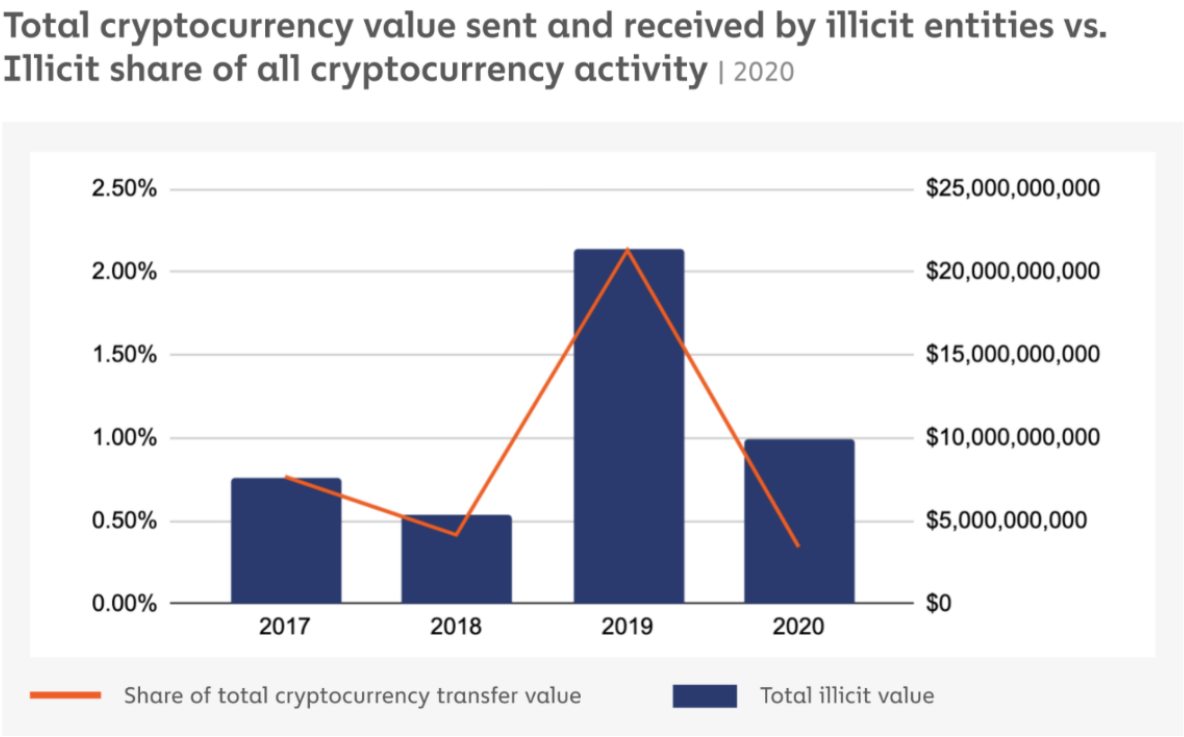


Figure 22: Illicit crypto transfers (chainanalysis)[587]

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

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

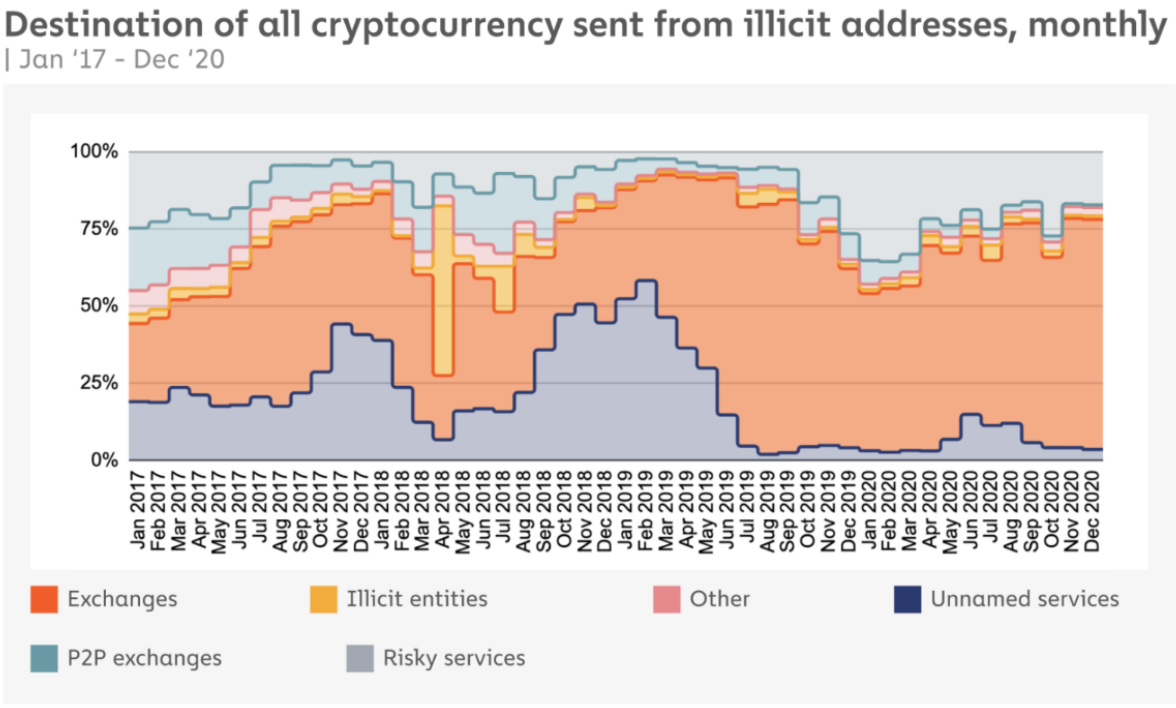


Figure 23: Illicit cryptocurrency transfer destinations by type. (chainanalysis)[588]

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[589] 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.

8.5 Summary

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. Global ransomware volumes continue to grow exponentially.

[588] https://go.chainalysis.com/2021-Crypto-Crime-Report.html
[589] https://www.reuters.com/technology/eu-tighten-rules-cryptoasset-transfers-2021-07-20/

Properties of cryptocurrencies have fuelled rising trends in ransomware to a degree. However, ransomware existed before cryptocurrencies and has used different payment methods in the past, so it alone is not an enabler. Recent ransomware-as-a-service models are probably the driving force behind the current trend.

Private communication methods play a key role in cybercrime and enabling the market ecosystem. While general public interest stagnates, as does the growth of the technologies enabling darknet and private avenues for cybercriminals, the cybercrime markets contain more impactful services and products than ever before.

While cybercriminals continue to scam each other online, the ecosystem has matured over the years to be more reliable. Reputation plays a key role in the markets, and cryptocurrencies continue to increase in popularity in the cybercrime space, too.

The nature of digital goods and services makes it easier to sell/provide and more challenging to fight against from the law enforcement side. Privacy online is a double-edged sword: while we all can appreciate the technologies developed for us to keep our privacy, it makes it increasingly difficult to fight against malicious users.

A recently proposed law by the European Commission to make cryptocurrency transactions traceable and anonymous wallets illegal may hinder gateways to fiat–cryptocurrency transactions of cybercriminals when such services are provided by organisations such as exchanges, but considering the peer-to-peer nature of cryptocurrencies, the effects on cybercrime may be small. Nevertheless, the initiative is a step in the right direction in terms of fighting the criminal use of cryptocurrencies.

All in all, cybercrime is looking like a growing field. Ransomware as a threat is particularly prevalent and increasing exponentially. Criminals are looking for mobile technologies for communication and an increasing amount of criminal funds are transferred and laundered via cryptocurrencies.

9 LEA involvement in countering cybercrime and dealing with its drivers

As laid out elsewhere, cybercrime, in many different forms, has become a growing technical challenge and security-related concern. Law-enforcement agencies (LEA) are struggling particularly with the aforementioned trends. This section sheds some light on the LEA perspective on cybercrime drivers, which is illustrated by briefly analysing (LEA) threat assessments and attempts to stem the tide of steadily growing cyberattacks. These proceedings are illustrated by casting light on the situation in Germany.

When it comes to the technological drivers of cybercrime, the German LEA community reported a drastic increase in the use of spam emails (up by 2.8 times in 2019 compared to 2018) that are mostly used to retrieve sensitive data (phishing), and explicitly warned of the use of cryptocurrencies and the dark web for cybercriminal purposes, Cybercrime-as-a-Service, malware, ransomware and distributed denial of service (DDoS) attacks (Bundeskriminalamt, 2020a). The most recent cybercrime report of the European Union Agency for Law Enforcement Cooperation corroborated the threat posed by the aforementioned developments. The ransomware issue and—albeit to a lesser extent—the malware and DDoS threats were especially emphasised (Europol, 2020).

Besides the steadily growing reliance on technological procedures, including the IT infrastructure, that provide cybercriminals with new opportunities to engage in criminal activities, cybercriminals have also become more sophisticated, which is a profound cause of concern for LEAs. Phishing since many years has been a cybercrime threat, which is constantly changing and adapting to the new reality. More specifically, phishing has been used for quite a while to steal identities, but in 2020 such stolen identities and further data that had been retrieved through phishing and social engineering were used to conduct illicit online payments by using mobile systems in Germany. That was a new type of cybercrime. Prior to 2020 the German LEAs had not observed the infringement of mobile payment services through stolen identities (Bundeskriminalamt, 2020a). Furthermore, so-called smishing activities have added another layer to the phishing dimension. In contrast with the latter, the former is relatively new. Whereas traditional phishing mostly uses spam emails as described above, smishing relies on fraudulent text messages that are shared with potential victims. The underlying logic is quite conclusive, considering that many Internet users have had bad experiences with spam emails and are wary of their dangers. Text messages, on the other hand, are usually viewed with much less scepticism.[590]

Cybercriminals have also adjusted their tactics in other cybercrime fields to maximise the impact of their activities, overcome countermeasures and avoid prosecution. As a result, the available malware has become extremely sophisticated. Moreover, it is partially offered for sale on the darknet. Besides the abovementioned issue of cybercrime-as-a-service, there is a particular class of malware that represents a service threat. Thanks to the darknet supply, even cybercriminals who do not have the skills or knowledge to conceptualise advanced malware programs may acquire and use them (Europol, 2020).

[590] Virgillito, D. 2021: Top 9 cybercrime tactics, techniques and trends in 2020: A recap, 08 February 2021, retrieved from: https://resources.infosecinstitute.com/topic/top-9-cybercrime-tactics-techniques-and-trends-recap/.

DDoS attacks, which have been observed for over 20 years now, could turn out to be particularly challenging for the years ahead, considering that cybercriminals have shown signs of exploiting the Internet of Things environment to enhance DDoS attacks (Europol, 2020). Recently, the European Union Agency for Law Enforcement Cooperation stipulated that those "who engage in DDoS attacks have adapted against increasingly robust protection measures. Instead of targeting high-value targets with massive volume attacks, attackers have shifted their focus on smaller organisations with less mature security apparatus. Downscaling their targets enable attackers to utilise volume more efficiently, and ensure maximum payout when the attacks are financially motivated", in the sense that defensive measures are much easier to overcome that way (Europol, 2020, p. 32).

For numerous reasons, these are highly worrisome developments in general and for LEAs in particular. As the European Union Agency for Law Enforcement Cooperation further concluded, one of the implications of the above-mentioned trends is that "it is increasingly challenging for possible cybercrime victims to avoid being subjected to such attacks. There is a growing imbalance between attackers and possible victims in the sense that the skill-set of the first requires very robust knowledge and efforts on the part of the latter. Obviously, this is driving cybercrime in the sense that the number of cybercrime incidents is virtually guaranteed to further increase if the aforementioned imbalance is not reversed, or at least successfully addressed" (Europol, 2020, p. 33).

While LEAs are mostly in charge of investigating crimes, including cybercrimes (in other words, they are used to getting involved after the incident), they are also very concerned about how to prevent the misuse of the above-mentioned technological tools. They have to confront increasingly advanced skills on the part of the attackers with inadequate resources and countermeasures on the part of possible victims. Frequently, cybersecurity expenses are still largely seen as a cost factor and not so much as a necessity. To the dismay of LEAs and other security experts, the business world, where short-term balance sheets may determine the fate of CEOs and board members, is still quite oblivious to the need to invest large sums in beefing up cybersecurity standards.[591]

The Covid-19 pandemic has not changed this dire situation for the better. On the contrary, "[t]he fast shift to telework made some companies 'alleviate' some of their IT security policies and some IT security responsibility has been transferred to the individual users, where varying levels of (or lack of) associated security training has created a new gap in security" (Europol, 2020, p. 25).

Against this backdrop, LEAs, their investigative duties notwithstanding, have a huge interest in raising awareness of the cybercrime threat. This issue was discussed by the CC-DRIVER LEA Working Group on Friday 11th June 2021, in a meeting organised by Valencia Local Police and attended by seven LEAs from 5 countries (Finland, Germany, Greece, Slovenia and Spain). In an expert conversation on best practices regarding the fight against cybercrime, LEA participants all agreed that raising awareness of the cyber threat was a key challenge. However, as mentioned above, public outreach is not the primary task of LEAs. The discussion revealed that the readiness to engage the public varied greatly among LEAs. Some of them are rather

[591] Schneier, B. 2021: Why Was SolarWinds So Vulnerable to a Hack?, The New York Times, 23 February 2021, retrieved from: https://www.nytimes.com/2021/02/23/opinion/solarwinds-hack.html.

reluctant to use social media, whereas the Spanish National Police Twitter account @Policia has 3.5 million followers.

Besides setting aside personnel and time to engage the public, conceptualising successful awareness raising campaigns is quite demanding for other reasons, too. Such outreach efforts often fail, or even cause more harm than good, because they do not manage to identify the proper target group and/or message (Fraustino & Ma, 2015; Christiano & Neimand, 2017). In other words, it does take some expertise in public communication in general and—at least currently—possibly the use of social media in particular to make a meaningful and effective contribution to raising awareness (let alone of an issue that is as complex as cybercrime).

Unfortunately, the LEA Working Group observed that numerous LEAs are having trouble recruiting highly qualified public relations experts/social media managers. The latter's expertise is in very high demand, making the job market very competitive for employers, whereas well-qualified potential employees can apply for numerous jobs. To make things worse, the public service in general, and LEAs in particular, can hardly compete with the private sector, where skilled cyber and social media experts can usually find far more lucrative jobs.

The need for capacity-building in the preventive realm notwithstanding, personnel shortages are also a profound issue when it comes to investigating cybercrime incidents. It goes without saying that both the increase in cybercrime incidents and their growing complexity require that LEA officials are entrusted with cybercrime portfolios in far greater numbers. Moreover, targeted and efficient cybercrime investigations require an even more complex and, presumably, rare scope of expertise than awareness raising efforts. The more cybercriminals adapt to the online environment, as described above, the more challenging it becomes to get hold of them, which makes cybercrime investigations even more demanding.

Having said that, there is light at the end of the tunnel in the sense that LEAs have started to double-down on the hiring of cybercrime personnel. Germany is a case in point. The Federal Criminal Police Office set up a new cybercrime department in April 2020, which replaced the "Group Cybercrime" that had been created in 2013. The latter's 100 staffers have been merged with the new department, which is envisaged to eventually have about 280 experts from all relevant sub-disciplines of the cybercrime issue, including forensic officers, analysts and IT experts with a wide range of expertise (Bundeskriminalamt, 2020b).

While this is a step in the right direction, it is obviously not sufficient to keep up with the growing cybercrime threat. This is well illustrated by the appallingly high number of cybercrime incidents. To put the abovementioned number of experts in context, some current cybercrime figures are discussed below, again with a focus on Germany, which the approximately 280 experts are supposed to keep safe (albeit not just by themselves).

In 2019 three fourths of German businesses reported that they had been subject to cybercrime. Moreover, the number of critical infrastructure attacks has skyrocketed. Between May 2019 and June 2020, critical infrastructure organisations in Germany reported 419 incidents, while in the previous year there had been only 252 such attacks. Most incidents were reported by the financial sector, closely followed by the IT and communication sectors (Bundesamt für Sicherheit in der Informationstechnik (BSI), 2020).

This presents a special challenge for the LEA community. While such critical infrastructure attacks occur far less often than other more common forms of cybercrime, their implications

can be spectacularly huge. A successful attack, i.e. on a major communication provider such as those that are running critical IT systems, may cause unprecedented panic. So, the cybercrime environment is not just driven by the abstract imbalance between attackers and possible victims: this imbalance also creates new opportunities to cause severe damage, which may easily attract an interest in taking advantage thereof on the part of cybercriminals. From an LEA perspective, such incidents are likely to be very hard to investigate, considering that cybercriminals engaging in such extraordinary cyberattacks are likely to be particularly skilled.

However, hiring skilled experts, as necessary as it is, is not going to be sufficient to address, let alone reduce the cybercrime threat. The reluctance on the part of the private sector to invest in protection measures has been discussed already. Unfortunately, there are further repercussions of an environment that rewards short-term profits, namely a clear and apparent reluctance to report cybercrime activities. Doing so may undermine the customers' belief in the company concerned, which gives the latter a clear incentive to sweep things under the rug. Moreover, the readiness to report cybercrime incidents to LEAs that in many ways are still understaffed also appears to have fallen victim to a catch-22 dilemma. "Victims may not see the value of doing so as law enforcement have limited resources to conduct investigations. Yet, reporting the crime can also help law enforcement in its quantitative justification to support the request for more resources" (Europol, 2020, p. 19).

Encouraging more transparency is going to be a profound challenge for LEAs. To be able to conduct investigations of all cybercrimes, such incidents need to be properly, comprehensively and quickly reported to LEAs. Moreover, thorough investigations are likely to require the support of the private sector victims. While awareness-raising initiatives may increase the sensitivity towards cybercrime, it appears that more robust efforts that ensure an institutional cooperation between LEAs and the private sector are necessary to meet all these challenges.

To guarantee that cybercrimes are fully reported and can be adequately investigated, all key players need to have a seat at the table. In Germany it has been decided to set up a special unit to meet this challenge. This unit, which is called National Cybercrime Cooperation Centre (NKC), is part of the above-mentioned cybercrime department. The NKC is responsible for cooperation with public authorities and private sector companies in this area of criminal phenomena. Additionally, the NKC is responsible for coordinating and liaising with the National Cyber Defence Centre, which comprises representatives of the Federal Office for Security in Information Technology, the Federal Office for the Protection of the Constitution, the Federal Office for Civil Protection and Disaster Relief, the Federal Police, the Bundeswehr, the Military Counterintelligence Service and the Customs Criminal Office. In this circle, security-relevant cyber incidents are jointly collected and evaluated (Bundeskriminalamt, 2020c).

Further engagement with the private sector takes place within the framework of the cybercrime department's administrative management of the federal state network of the Central Focal Points Cybercrime (ZAC). The ZAC network was set up to provide companies affected by cybercrime with direct contact with the federal and state police services' relevant cybercrime units (Bundeskriminalamt, 2020c).

The cybercrime department's private sector engagement is completed by the department's Quick Reaction Force (QRF), which is a 24/7 "first assault" call unit. The QRF initiates the first non-deferred criminal procedural measures in the event of cyberattacks on critical

infrastructure or federal facilities (Bundeskriminalamt, 2020c). While everybody might be subject to cybercrime attacks, the scope of the threat, especially in view of the potentially disastrous consequences, posed by attacks on critical infrastructure providers requires that special attention is paid to coordinating cybercrime responses to such incidents between LEAs and other key players within and outside of government.

While further action may be necessary on this front, too, the abovementioned measures are quite illustrative of the huge concern on the part of LEAs regarding the need to team up with other players to address the cybercrime threat. Reliable cooperation with the private sector is also required to ensure that another essential challenge to the investigation of cybercrime incidents is fully addressed, namely the use of cryptocurrencies, especially within the framework of extortion activities. Cybercriminals try to take advantage of the anonymity that cryptocurrency providers usually attempt to provide to their customers; this, however, is now subject to regulation on the European level in the form of the Fifth Anti-Money-Laundering Directive. Further deepening the cooperation with cryptocurrency providers may increase the odds of successfully concluding cybercrime investigations (Europol, 2020, p. 17-18).

Any discussion of the current cybercrime landscape, let alone of the pitfalls of investigating cybercrime incidents, would be incomplete without addressing the need for international cooperation. Notwithstanding the necessity for the abovementioned countermeasures that have been taken within the framework of the German Federal Criminal Police Office's cybercrime department, they are limited to the national realm. Given the transnational nature of cybercrime, however, there is an obvious need for international law enforcement cooperation. Again, the cybercrime department nicely illustrates this point, as it coordinates the international exchange of information.

The importance of international collaboration is further emphasised by a major LEA breakthrough: namely, the takedown of the world's largest illegal marketplace on the dark web, the DarkMarket, by German LEAs on 11 January 2021. The seizure of the DarkMarket and the arrest of the suspected operator by German police resulted from an international law enforcement operation, including agencies from Australia, Denmark, Moldova, Ukraine, the UK and the USA, and Europol. More than 20 servers were seized in Moldova and Ukraine. Almost 500,000 users and more than 2400 sellers had been active on the DarkMarket, conducting over 320,000 transactions, with a money transfer of more than 140 million EUR. The vendors on the DarkMarket had mainly traded all kinds of drugs and sold counterfeit money, stolen or fake credit card details, anonymous SIM cards and malware (Europol, 2021b).

10 Conclusion

In this document we have presented the main technical and human drivers of cybercrime. On the technical side, we have identified several drivers: (i) ***buggy software*** that can be compromised by tech-savvy cybercriminals, (ii) ***"smart" devices*** that provide more opportunities for attacks, (iii) ***anonymity*** made possible by VPNs and anonymising networks, (iv) ***cryptocurrencies*** that facilitate the anonymous transfer of (illegal) money, and (v) the provision of ***cybercrime "as-a-service"*** that provides easy access to cybercrime services for all your aspiring cybercriminals. On the human side, we have identified how key academic theories might be applied to the world of cyberspace and aid global understandings of human drivers of cybercrime and cyberdelinquency, while acknowledging the logistical obstacles afforded by the far-reaching web in the endeavour to tackle cybercrime and cyberdelinquency. The Covid-19 pandemic has led to unprecedented volumes of online audiences and, in turn, the world has witnessed surges in cybercrime worldwide. While there is little literature available to investigate the malicious and callous underpinnings of profiting financially from a global pandemic, we have attempted to begin to touch on some of these questions, specifically relating to the human factors involved in cybercrime perpetration. We highlighted the diversity of cybercriminals, especially in relation to motive, but also in their other characteristics. Approaches to profiling cybercriminals may be largely dependent on the crime itself, or the level of skill involved, the ethos of virtual subcultures and, of course, the multitude of human factors that are at play. The human factors of cybercrime are complex and nuanced, yet are crucial to grasp. Applying a multidisciplinary approach is key.

Our findings suggest that these drivers of cybercrime are probably not going to go away easily. Some of them will, by popular demand, continue to proliferate and in this way to be (inadvertently) a springboard for cybercrime. Indeed, the "smart" devices and the IoT will continue to penetrate our everyday lives, thus enlarging the attack surface and allowing more opportunities for cybercriminals. Some others, such as the use of anonymisation tools, dealing with the sensitive area of human rights (such as privacy) will be very difficult to change without major human rights debates, and possibly compromises. Other drivers, such as those referring to cryptocurrencies for example, may be mitigated through policy and regulation, and thus may reduce the thrust they provide to cybercrime, although it is not clear how much time and effort it will take until this happens.

All in all, it seems that several of the identified trends will continue to have a strong presence in the near future, and the response to cybercrime will be increasingly challenging. To mitigate this challenge effectively, we trust that the combination of research, innovation, and technological development through a multidisciplinary approach is of paramount importance.

11 References

Adesina, O. S. (2017). Cybercrime and poverty in Nigeria. *Canadian social science*, 13(4), 19-29.

Agnew, R. (1992). Foundation for a general strain theory of crime and delinquency. Criminology, 30(1), 47-88, DOI:10.1111/j.1745-9125.1992.tb01093.x.

Ahlgrim, Billea, and Cheryl Terrance. "Perceptions of cyberstalking: Impact of perpetrator gender and cyberstalker/victim relationship." *Journal of interpersonal violence* 36, no. 7-8 (2021): NP4074-NP4093.

Aiken, M. P. (2016). The Cyber Effect. New York. Random House, Spiegel & Grau.

Aiken, M. P. (2018) Mass Killing and Technology: The Hidden Links. Retrieved from https://debugged.wilsoncenter.org/mass-killing-and-technology-the-hidden-links-b434ba6825e1

Aiken, M., Davidson, J., & Amann, P. (2016). Youth Pathways into Cybercrime. London: Paladin Capital Group.

Aiken, M.P., Farr, R., & Witschi, D. (2022) Cyberchondria, Coronavirus and Cybercrime: A Perfect Storm in H. Aker & M.P Aiken (Eds) Cyberchondria, Health Literacy, and the Role of Media in Society's Perception of Medical Information. IGI Global. https://www.igi-global.com/chapter/cyberchondria-coronavirus-and-cybercrime/293431

Aiken, M. P., & Mc Mahon, C. (2014). The CyberPsychology of Internet Facilitated Organised Crime. The Hague: EUROPOL.

Akhgar, B., Staniforth, A., & Bosco, F. (Eds.). (2014). Cyber crime and cyber terrorism investigator's handbook. Syngress.

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.

Akdemir, N., & Lawless, C. (2020). Exploring the Human Factor in Cyber-enabled and Cyber-dependent Crime Victimisation: A Lifestyle Routine Activities Approach. Internet Research, 30(6), 1665-1687, DOI:10.1108/INTR-10-2019-0400.

Akdemir, N., Sungur, B., & Başaranel, B. U. (2020). Examining the Challenges of Policing Economic Cybercrime in the UK. Güvenlik Bilimleri Dergisi (International Security Congress Special Issue), Özel Sayı, 111-132.

Almansoori, A., Alshamsi, M., Abdallah, S., & Salloum, S. A. (2021, June). Analysis of Cybercrime on Social Media Platforms and Its Challenges. In The International Conference on Artificial Intelligence and Computer Vision (pp. 615-625). Springer, Cham.

Althaus, D., & Baumann, T. (2020). Reducing long-term risks from malevolent actors. Publications of Center of Long Term Risk.

Al Mutawa, N., Bryce, J., Franqueira, V. N., & Marrington, A. (2015). Behavioural evidence analysis applied to digital forensics: an empirical analysis of child pornography cases using P2P networks. *2015 10th International Conference on Availability, Reliability and Security* (pp. 293-302). Piscataway, NJ: IEEE.

Anderson, P., Zuo, Z., Yang, L., & Qu, Y. (2019, June). An Intelligent Online Grooming Detection System Using AI Technologies. In 2019 IEEE International Conference on Fuzzy Systems (FUZZ-IEEE) (pp. 1-6). IEEE.

Andrews, L., Holloway, M., & Massoglia, D. (2015). Digital peepholes: Remote activation of webcams: Technology, law and policy. The Institute for Science, law and technology.

Aneke, S. O., Nweke, E. O., Udanor, C. N., Ogbodo, I. A., Ezugwu, A. O., Uguwishiwu, C. H., & Ezema, M. E. (2020). Towards Determining Cybercrime Technology Evolution in Nigeria. International Journal of Lates Technology in Engineering, Management and Applied Science, ix, 37-43.

Attrill-Smith, A., & Wesson, C. (2020). The Psychology of Cybercrime. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 653-678.

Barlett, C. P., Gentile, D. A., Chng, G., Li, D., & Chamberlin, K. (2018). Social media use and cyberbullying perpetration: A longitudinal analysis. Violence and gender, 5(3), 191-197.

Beccaria, C. (1963). On crimes and punishments (introduction by H. Paolucci, Trans.). New York: Macmillan.

Becker, P. J., Byers, B., & Jipson, A. (2000). The contentious American debate: the first amendment and Internet-based hate speech. International Review of Law, Computers & Technology, 14(1), 33-41.

Benjamin, V., Li, W., Holt, T., & Chen, H. (2015, May). Exploring threats and vulnerabilities in hacker web: Forums, IRC and carding shops. I*n 2015 IEEE international conference on intelligence and security informatics (ISI)* (pp. 85-90). IEEE.

Berger, J. M., & Morgan, J. (2015). The ISIS Twitter Census: Defining and describing the population of ISIS supporters on Twitter.

Berry, M. J., and S. L. Bainbridge (2017). "Manchester's Cyberstalked 18-30s: Factors Affecting Cyberstalking". *Advances in Social Sciences Research Journal* 4 (18). https://doi.org/10.14738/assrj.418.3680.

Bertola, F. (2020). Drug trafficking on Darkmarkets: How cryptomarkets are changing drug global trade and the role of organized crime. *American Journal of Qualitative Research*, 4(2), 27-34.

Bishop, J. (2014). Dealing with internet trolling in political online communities: Towards the this is why we can't have nice things scale. International Journal of E-Politics (IJEP), 5(4), 1-20.

Bishop, P. (2020). Legislative Frameworks: The United Kingdom. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 281-304.

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

Block, J. (2008). Issues for DSM-V: Internet addiction. American Journal of Psychiatry, 165(3), 306–307, DOI:10.1176/appi.ajp.2007.07101556.

Bocij, P. (2006). *The Dark Side of the Internet: Protecting Yourself and Your Family from Online Criminals* . Westport, CT: Praeger

Bonilla, T., & Mo, C. (2019). The evolution of human trafficking messaging in the United States and its effect on public opinion. *Journal of Public Policy*, 39(2), 201-234. doi:10.1017/S0143814X18000107

Book, A., Visser, B. A., Blais, J., Hosker-Field, A., Methot-Jones, T., Gauthier, N. Y., … D'Agata, M. T. (2016). Unpacking more "evil": What is at the core of the dark tetrad? Personality and Individual Differences, 90, 269–272. https://doi.org/10.1016/j.paid.2015.11.009.

Bouché, V. (2015). A report on the use of technology to recruit, groom and sell domestic minor sex trafficking victims.

Bossler A., Berenblumb, T., (2019) Introduction: new directions in cybercrime research, Journal of Crime and Justice, Vol 42, NO. 5, 495–499 https://doi.org/10.1080/0735648X.2019.1692426

Brenner, S. (2007). Cybercrime: Re-thinking crime control strategies. In Y. Jewkes (Ed.), Crime online (pp. 12–28). Cullompton, United Kingdom: Willan Publishing.

Brewer, R. C., Cale, J., Goldsmith, A. J., & Holt, T. (2018). Young people, the Internet, and emerging pathways into criminality: A study of Australian adolescents. International Journal of Cyber Criminology, 12(1), 115-132, DOI:10.5281/zenodo.1467853.

Brown, W. M., Hazraty, S., & Palasinski, M. (2019). Examining the dark tetrad and its links to cyberbullying. Cyberpsychology, Behavior, and Social Networking, 22(8), 552-557.

Buckels, E. E., Jones, D. N., & Paulhus, D. L. (2013). Behavioral confirmation of everyday sadism. Psychological Science, 24, 2201–2209, http://dx.doi.org/10.1177/0956797613490749.

Budapest Convention on Cybercrime Classification. (2001).

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.

Bundesamt für Sicherheit in der Informationstechnik (BSI). (2020). Die Lage der IT-Sicherheit in Deutschland 2020, Bonn 2020 [Federal Office for Information Security: The State of IT Security in Germany in 2020], Available at: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2020.pdf?__blob=publicationFile&v=2.

Bundeskriminalamt. (2020a). Bundeslagebild Cybercrime 2019. Available at: https://www.bka.de/SharedDocs/Downloads/DE/Publikationen/JahresberichteUndLagebilder/Cybercrime/cybercrimeBundeslagebild2019.html?nn=28110

Bundeskriminalamt. (2020b). Bundeskriminalamt stärkt die Cybercrime bekämpfung. Available at: https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2020/Presse2020/200401_pmAbteilungCC.html

Bundeskriminalamt. (2020c). Abteilung Cybercrime. Available at: https://www.bka.de/DE/DasBKA/OrganisationAufbau/Fachabteilungen/Cybercrime/cybercrime_node.html

Buschman, J., Wilcox, D., Krapohl, D., Oelrich, M., & Hackett, S. (2010). Cybersex offender risk assessment. An explorative study. Journal of sexual aggression, 16(2), 197-209.

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).

Caines, A., Pastrana, S., Hutchings, A., & Buttery, P. J. (2018). Automatically identifying the function and intent of posts in underground forums. Crime Science, 7(1), 1-14.

Cameron, M., & Laycock, G. (2002). Crime prevention in Australia. In A. Graycar, & P. Grabowsky, The Cambridge handbook of Australian criminology. (pp. 313–331).

Melbourne: Cambridge University Press. Retrieved from E4J University Module Series: Crime Prevention and Criminal Justice: https://www.unodc.org/e4j/en/crime-prevention-criminal-justice/module-2/key-issues/2a--detailed-explanation-of-tonry-and-farringtons-typology.html

Caneppele, S. & Aebi, M. F. (2019). Crime Drop or Police Recording Flop? On the Relationship between the Decrease of Offline Crime and the Increase of Online and Hybrid Crimes. *Policing: A Journal of Policy and Practice*, 13(1), 66–79.

Carrabine E, Cox P, Lee M, Plummer K & South, N (2009). Criminology: a sociological introduction, second edition, Routledge, New York. Available at: https://www.hrstud.unizg.hr/_download/repository/Eamonn_Carrabine,_Maggy_Lee,_Nigel_South,_Pam_Cox,_Ken_Plummer_Criminology_A_Sociological_Introduction__2009.pdf

Carlton, A. (2020). Sextortion: The Hybrid "Cyber-Sex" Crime. *North Carolina Journal of Law and Technology*, 21(3), 177-215.

Carney, M. a. (2004). The Trojan Made Me Do It: A First Step in Statistical Based Computer Forensics Event Reconstruction. International Journal of Digital Evidence.

Carr, A. (2004). Internet traders of child pornography and other censorship offenders in New Zealand. Wellington: Department of Internal Affairs. https://www.dia.govt.nz/diawebsite.nsf/wpg_URL/Resource-material-Our-Research-and-Reports-Internet-Traders-of-Child-Pornography-and-other-Censorship-Offenders-in-New-Zealand?OpenDocument

Center for Health and Justice. (2013). A national survey of criminal justice diversion programs and initiatives.

Chatterjee, R., Doerfler, P., Orgad, H., Havron, S., Palmer, J., Freed, D., . . . Ristenpart, T. (2018). The spyware used in intimate partner violence. 2018 IEEE Symposium on Security and Privacy (SP) (pp. 441-458). San Francisco, CA: IEEE.

Christiano, A., & Neimand, A. (2017). Stop raising awareness already. *Stanford Social Innovation Review*, 15(2), 34-41.

Ciardhuáin, S. Ó. (2004). An Extended Model of Cybercrime Investigations. International Journal of Digital Evidence, 3(1).

Citron, D. K. (2015). Spying Inc. *Wash. & Lee L. Rev.*, 72, 1243.

Clark, M. (2021, May 10). Colonial Pipeline hackers apologize, promise to ransom less controversial targets in future. Retrieved July 31, 2021, from The Verge: https://www.theverge.com/2021/5/10/22428996/colonial-pipeline-ransomware-attack-apology-investigation

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

Cohen, L. E., & Felson, M. (1979). Social change and crime rate trends: A routine activity approach. American sociological review, 44, 588-608, DOI: 10.2307/2094589.

Collier, B., Horgan, S., Jones, R., Shepard, L., (2020), "The implications of the COVID-19 pandemic for cybercrime policing in Scotland: A rapid review of the evidence and future considerations" Research evidence in Policing: Pandemics, The Scottish Institute for Policing Research, Issue 1.

Coluccia, A., Pozza, A., Ferretti, F., Carabellese, F., Masti, A., & Gualtieri, G. (2020). Online romance scams: Relational dynamics and psychological characteristics of the victims

and scammers. A scoping review. *Clinical Practice and Epidemiology in Mental Health: CP & EMH*, *16*, 24–35, doi: 10.2174/1745017902016010024.

Connolly, Irene., Palmer, Marion,. Barton, Hannah,. Kirwan, Grainne. (2016). Introduction to Cyberpsychology. An Introduction to Cyberpsychology (pp. 3-14). New York, NY: Routledge.

Conway, M. (2006). Terrorism and the Internet: New media—New threat?. Parliamentary Affairs, 59(2), 283-298.

Cook, C., Schaafsma, J., & Antheunis, M. (2018). Under the bridge: An in-depth examination of online trolling in the gaming context. New Media & Society, 20(9), 3323-3340.

Cooke, E., Jahanian, F., & McPherson, D. (2005). The Zombie Roundup: Understanding, Detecting, and Disrupting Botnets. *SRUTI*, 5, 6-6.

Costello, M., & Hawdon, J. (2020). Hate speech in online spaces. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 1397-1416.

Costello, M., Hawdon, J., Ratliff, T., & Grantham, T. (2016). Who views online extremism? Individual attributes leading to exposure. Computers in Human Behavior, 63, 311-320.

Council of Europe . (2001). Convention on cybercrime. European Treaty Series, No. 185, 1-25.

Crawford, J. (2021). The Computer Misuse Act and Hackers: A review of those convicted under the Act. Egham, Surrey: Information Security Group, Royal Holloway University of London.

Cross, C. (2019). Online fraud. In Oxford Research Encyclopedia of Criminology and Criminal Justice.

Cross, C. (2020). Romance Fraud. In T. J. Holt, & A. M. Bossler, The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 917-937). Cham, Switzerland: Springer International Publishing AG.

Daigle, L. E., Cullen, F. T., & Wright, J. P. (2007). Gender differences in the predictors of juvenile delinquency: Assessing the generality-specificity debate. *Youth Violence and Juvenile Justice*, *5*(3), 254-286.

Daniels, J. (2009). Cyber racism: White supremacy online and the new attack on civil rights. Rowman & Littlefield Publishers.

Demetis, D. S. (2020). Breaking bad online: A synthesis of the darker sides of social networking sites. European Management Journal, 38(1), 33-44, https://doi.org/10.1016/j.emj.2019.12.013.

Dingledine, R., Mathewson, N., & Syverson, P. (2004). Tor: The Second-Generation Onion Router. *USENIX Security Symposium*.

Dawson, M. (2020). CYBERCRIME: INTERNET DRIVEN ILLICIT ACTIVITIES AND BEHAVIOR. *Land Forces Academy Review*, 25(4), 356-362.

Denning, D. E. (2000). Cyberterrorism: Testimony before the special oversight panel on terrorism committee on armed services US House of Representatives. Focus on Terrorism, 9, 71-76.

Donaldson, S., Davidson, J., & Aiken, M. (2020). Safer technology, safer users: The UK as a world-leader in Safety Tech.

Dreßing, H., Bailer, J., Anders, A., Wagner, H., & Gallas, C. (2014). Cyberstalking in a large sample of social network users: Prevalence, characteristics, and impact upon victims. *Cyberpsychology, Behavior, and Social Networking*, 17(2), 61-67.

Douglas, K. M., McGarty, C., Bliuc, A. M., & Lala, G. (2005). Understanding cyberhate: Social competition and social creativity in online white supremacist groups. Social Science Computer Review, 23(1), 68-76.

Du, P. Y., Zhang, N., Ebrahimi, M., Samtani, S., Lazarine, B., Arnold, N., ... & Chen, H. (2018, November). Identifying, collecting, and presenting hacker community data: Forums, IRC, carding shops, and DNMs. In *2018 IEEE international conference on intelligence and security informatics (ISI)* (pp. 70-75). IEEE.

Duggan, M. (2017). Online harassment 2017. The Pew Research Center. https://www.pewresearch.org/internet/2017/07/11/online-harassment-2017/

Dupont, B., Côté, A. M., Boutin, J. I., & Fernandez, J. (2017). Darkode: Recruitment patterns and transactional features of "the most dangerous cybercrime forum in the world". American Behavioral Scientist, 61(11), 1219-1243.

ECPAT International. (2016). Terminology Guidelines for the Protection of Children from Sexual Exploitation and Sexual Abuse. Luxembourg: ECPAT.

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 (2019). Internet organised crime threat assessment. Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2019

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

Europol (2021). Serious and Organised Crime Threat Assessment.

Europol (2021b). DarkMarket: world's largest illegal dark web marketplace taken down. Available at: https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down

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/

F-SECURE (2021). Ransomware 2.0, automated recon, supply chain attacks, and other trending threats. Available at https://blog-assets.f-secure.com/wp-content/uploads/2021/03/30120359/attack-landscape-update-h1-2021.pdf

Fairbairn, J., & Spencer, D. (2018). Virtualized violence and anonymous juries: Unpacking steubenville's "big red" sexual assault case and the role of social media. Feminist criminology, 13(5), 477-497.

Fansher, Ashley K., and Ryan Randa (2019). "Risky social media behaviors and the potential for victimization: A descriptive look at college students victimized by someone met online." *Violence and gender* 6, no. 2: 115-123.

Ferreira, A. (2018). Why ransomware needs a human touch. 2018 International Carnahan Conference on Security Technology (ICCST) (pp. 1-5). Montreal, QC, Canada: IEEE.

Federal Criminal Police Office. (2021). Cybercrime: Bundeslagebild 2020.

Finklea, Kristin & Theohary, C.A.. (2013). Cybercrime: Conceptual issues for congress and U.S. law enforcement. Cybercrime: Conceptualized and Codified. 1-27.

Fissel, E. R., & Reyns, B. W. (2020). The aftermath of cyberstalking: School, work, social, and health costs of victimization. *American Journal of Criminal Justice*, 45(1), 70–87. https://doi.org/10.1007/s12103-019-09489-1

Frank, R., & Mikhaylov, A. (2020). Beyond the 'Silk Road': Assessing Illicit Drug Marketplaces on the Public Web. In *Open Source Intelligence and Cyber Crime* (pp. 89-111). Springer, Cham.

Fraustino, J. D., & Ma, L. (2015). CDC's use of social media and humor in a risk campaign—"Preparedness 101: Zombie Apocalypse". *Journal of Applied Communication Research*, 43(2), 222-241. doi: 10.1080/00909882.2015.1019544.

Ganesan, M., & Mayilvahanan, P. (2017). Cyber Crime Analysis in Social Media Using Data Mining Technique. International journal of pure and applied mathematics, 116(22), 413-424.

Genlin, L., & Baker, D. J. (2020). Criminalising cybercrime facilitation by omission and its remote harm form in China. In *Artificial Intelligence and the Law* (pp. 126-155). Routledge.

Goldsmith, A., & Wall, D. S. (2019). The seductions of cybercrime: Adolescence and the thrills of digital transgression. European Journal of Criminology, 1-20, DOI:10.1177/1477370819887305.

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

Goode, E. (2015). Deviance, Crime and. In G. Ritzer, The Blackwell Encyclopedia of Sociology (p. DOI: 10.1002/9781405165518.wbeosd042.pub2). New Jersey: John Wiley & Sons, Ltd.

Gordon, S., & Ford, R. (2006). On the definition and classification of cybercrime. Journal in Computer Virology, 2(1), 13–20.

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

Graham, R. (2020). Race, Social Media, and Deviance. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 67-90.

Grant, M. J., & Booth, A. (2009). A typology of reviews: an analysis of 14 review types and associated methodologies. Health Information and Libraries Journal, 26, 91–108.

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

Hadzhidimova, L. I., & Payne, B. K. (2019). The profile of the international cyber offender in the US. International Journal of Cybersecurity Intelligence & Cybercrime, 2(1), 40-55.

Hay, C., & Ray, K. (2020). General Strain Theory and Cybercrime. In T. J. Holt, & A. M. Bossler, The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 583-600, DOI:10.1007/978-3-319-90307-1_21-1). New York: Springer International Publishing AG.

Hawdon, J., & Costello, M. (2018). Themes in the prognostic, diagnostic and motivational frames of hate groups. American Society of Criminology. November 17. Atlanta.

Heikkilä, M., & Cerulus, L. (2020, October 26). Hacker seeks to extort Finnish mental health patients after data breach. Retrieved July 31, 2021, from Politico: https://www.politico.eu/article/cybercriminal-extorts-finnish-therapy-patients-in-shocking-attack-ransomware-blackmail-vastaamo/

Heimer, K., & De Coster, S. (2001). Crime and Gender. In N. J. Smelser, & P. B. Baltes, *International Encyclopedia of the Social & Behavioural Sciences* (pp. 2918-2921). Oxford: Elsevier Science Ltd.

Heirman, W., & Walrave, M. (2012). Predicting adolescent perpetration in cyberbullying: An application of the theory of planned behavior. *Psicothema*, *24*(4), 614-620. PMID: 23079360.

Henry, N., & Flynn, A. (2020). Image-Based Sexual Abuse: A Feminist Criminological Approach. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 1109-1130.

Van Heugten, L., Bicker Caarten, A., & Merkle, O. (2021). Giving Up Your Body to Enter Fortress Europe: Understanding the gendered experiences of sextortion of Nigerians migrating to the Netherlands (No. 2021-050). United Nations University-Maastricht Economic and Social Research Institute on Innovation and Technology (MERIT).

Hinduja, S., & Patchin, J. W. (2014). Bullying beyond the schoolyard: Preventing and responding to cyberbullying. Corwin press.

Holt, K., & Liggett, R. (2020). Revenge Pornography. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 1131-1149.

Holt, T. J. (2013). Examining the forces shaping cybercrime markets online. *Social Science Computer Review*, 31(2), 165-177. doi: 10.1177/0894439312452998.

Holt, T. J. (2020a). Computer Hacking and the Hacker Subculture. In T. J. Holt, & A. M. Bossler, The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 725-742, DOI:10.1007/978-3-319-78440-3_31 725). New York: Springer International Publishing AG.

Holt, T. J. (2020b). Subcultural Theories of Crime. In T. Holt, & B. A, The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 513-526, DOI:10.1007/978-3-319-78440-3_19). Cham, Switzerland: Palgrave Macmillan.

Holt, T. J. (2020c). The Palgrave Handbook of International Cybercrime and Cyberdeviance. Cham: Palgrave Macmillan.

Holt, T. J., Navarro, J. N., & Clevenger, S. (2020). Exploring the moderating role of gender in juvenile hacking behaviors. *Crime & Delinquency, 66*(11), 1533-1555.

Holt, T. J., Smirnova, O., & Chua, Y. T. (2016). Exploring and estimating the revenues and profits of participants in stolen data markets. *Deviant Behavior*, 37(4), 353-367. doi: 10.1080/01639625.2015.1026766.

Holt, T. J., van Wilsem, J., van de Weijer, S., & Leukfeldt, R. (2020). Testing an integrated self-control and routine activities framework to examine malware infection victimization. *Social Science Computer Review*, *38*(2), 187-206.

Howitt, D. D. (2009). Introduction to Forensic and Criminal Psychology. Loughborough, UK: Pearson Education.

Huang, K., Siegel, M., & Madnick, S. (2018). Systematically understanding the cyber attack business: A survey. ACM Computing Surveys (CSUR), 51(4), 1-36.

Hutchings, A., & Collier, B. (2019). Inside out: Characterising cybercrimes committed inside and outside the workplace. In 2019 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (pp. 481-490). IEEE.

Hutchings, A., & Pastrana, S. (2019). Understanding eWhoring. 2019 IEEE European Symposium on Security and Privacy (EuroS&P) (pp. 201-214). Stockholm, Sweden: IEEE.

Hutchings, A., & Chua, Y. T. (2016). Gendering cybercrime. In Cybercrime through an interdisciplinary lens (pp. 181-202). Routledge.

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.

INTERPOL. (2020). Cybercrime: Covid-19 Impact, Lyon, France. Available at: https://www.interpol.int/content/download/15526/file/COVID-19%20Cybercrime%20Analysis%20Report-%20August%202020.pdf

ITU. (2009). Series X: Data Networks, Open System Communications and Security, Telecommunication security: Overview of cybersecurity. International Telecommunication Union.

Jeong, J. K., Mihelcic, J., Oliver, G., & Rudolph, C. (2019). Towards an improved understanding of human factors in cybersecurity. *EEE 2019 : Proceedings of the 1st International Conference on Trust, Privacy and Security in Intelligent Systems and Applications (TPS) & the 5th International Conference on Collaboration and Internet Computing (CIC)* (pp. 338-345, https://doi.org/10.1109/CIC48465.2019.00047). Piscataway, NJ: IEEE.

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

Joinson, A. N. (2001). Self-disclosure in computer-mediated communication: The role of self-awareness and visual anonymity. European journal of social psychology, 31(2), 177-192, DOI:10.1002/ejsp.36.

Jokic-Begic, N., Lauri Korajlija, A., & Mikac, U. (2020). Cyberchondria in the age of COVID-19. *PLoS One*, *15*(12), e0243704. doi:10.1371/journal.pone.0243704 PMID:33332400

Jonason, P. K., Slomski, S., & Partyka, J. (2012). The dark triad at work: How toxic employees get their way. Personality and individual differences, 52(3), 449–453.

Jordan, T., & Taylor, P. A. (1998). A Sociology of Hackers. The Sociological Review, 46(4), 757-81, DOI:10.1111/1467-954X.00139.

Joseph, L. (n.d.). Voyeuristic Disorder DSM-5 302.82 (F65.3). Retrieved August 1, 2021, from Theravive: https://www.theravive.com/therapedia/voyeuristic-disorder-dsm--5-302.82-(f65.3)

Kadlecová, L. (2015). Russian-speaking cybercrime: reasons behind its success. *Eur Rev Organised Crime*, 2(2), 104-121.

Kaylor, L., & Jeglic, E. L. (2021). Non-contact Paraphilic Disorders and Offending. In L. A. Craig, & R. M. Bartels, Sexual Deviance: Understanding, Assessing and Managing Deviant Sexual Interests and Paraphilic Disorders (p. 171). Hoboken, NJ: John Wiley & Sons Ltd.

Kaur, Puneet, Amandeep Dhir, Anushree Tandon, Ebtesam A. Alzeiby, and Abeer Ahmed Abohassan. "A systematic literature review on cyberstalking. An analysis of past achievements and future promises." *Technological Forecasting and Social Change* 163 (2021): 120426.

Keipi, T., Näsi, M., Oksanen, A., & Räsänen, P. (2016). Online hate and harmful content: Cross-national perspectives (p. 154). Taylor & Francis.

Kennedy, G., McCollough, A., Dixon, E., Bastidas, A., Ryan, J., Loo, C., & Sahay, S. (2017, August). Technology solutions to combat online harassment. In Proceedings of the first workshop on abusive language online (pp. 73-77).

Kennedy, J. P. (2020). Counterfeit products online. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 1001-1024.

Kemp, S., Miró-Llinares, F. & Moneva, A. (2020). The Dark Figure and the Cyber Fraud Rise in Europe: Evidence from Spain. *European Journal on Criminal Policy and Research* 26, 293–312.

Khoo, C., Robertson, K., & Deibert, R. (2019). Installing Fear: A Canadian Legal and Policy Analysis of Using, Developing, and Selling Smartphone Spyware and Stalkerware Applications. Toronto: Citizen Lab.

King, Z. M., Henshel, D. S., Flora, L., Cains, M. G., Hoffman, B., & Sample, C. (2018). Characterizing and measuring maliciousness for cybersecurity risk assessment. Frontiers in psychology, 9(39), 1-19, doi: 10.3389/fpsyg.2018.00039.

Kirwan, G. (2010). Cyberpsychology: An overview of emerging research in emerging environments. The Irish Journal of Psychology, 31, 157–172.

Kirwan, G., & Power, A. (2012). The Psychology of Cyber Crime: Concepts and Principles: Concepts and Principles. Igi Global.

Kirwan, G., & Power, A. (2013). Cybercrime: The psychology of online offenders. Cambridge University Press.

Kohlberg, L & Hersh, R (2009). Moral development: A review of the theory, Theory Into Practice, Volume 16, Taylor and Francis Online. Available at: https://doi.org/10.1080/00405847709542675

Kokolaki, E., Daskalaki, E., Psaroudaki, K., Christodoulaki, M., & Fragopoulou, P. (2020). Investigating the dynamics of illegal online activity: The power of reporting, dark web, and related legislation. Computer Law & Security Review, 38, 105440.

Kranenbarg, M. W., & Leukfeldt, R. (Eds.). (2021). *Cybercrime in Context: The human factor in victimization, offending, and policing*. (pp. 175-194) Springer Nature.

Kranenbarg, M. W., Ruiter, S., Van Gelder, J. L., & Bernasco, W. (2018). Cyber-offending and traditional offending over the life-course: An empirical comparison. *Journal of developmental and life-course criminology*, *4*(3), 343-364. https://doi.org/10.1007/s40865-018-0087-8

Krone, T. (2004). A typology of online child pornography offending. *Trends and issues in crime and criminal justice*, *279*, 1-6.

Kshetri, N., & DeFranco, J. F. (2020). The Economics of Cyberattacks on Brazil. *Computer*, 53(9), 85-90.

Lauger, T. R., & Densley, J. A. (2018). Broadcasting badness: Violence, identity, and performance in the online gang rap scene. Justice Quarterly, 35(5), 816-841.

Lauger, T. R., Densley, J. A., & Moule, R. K. (2020). Social media, strain, and technologically facilitated gang violence. The Palgrave handbook of international cybercrime and cyberdeviance, 1375-1395.

Lee, J. R., & Holt, T. J. (2020). Assessing the Factors Associated With the Detection of Juvenile Hacking Behaviors. Frontiers in Psychology, 11, 840.

Lee, A. F., Li, N. C., Lamade, R., Schuler, A., & Prentky, R. A. (2012). Predicting hands-on child sexual offenses among possessors of Internet child pornography. Psychology, Public Policy, and Law, 18(4), 644.

Lee, M. C., Vajiac, C., Kulshrestha, A., Levy, S., Park, N., Jones, C., ... & Faloutsos, C. (2021). INFOSHIELD: Generalizable Information-Theoretic Human-Trafficking Detection. In 2021 IEEE 37th International Conference on Data Engineering (ICDE) (pp. 1116-1127). IEEE.

Lee, K. S., & Wei, H. (2019). Design Interventions against Trolling in Social Media: A Classification of Current Strategies Based on Behaviour Change Theories.

Lenhart, A., Ybarra, M., & Price-Feeney, M. (2016). Nonconsensual image sharing: one in 25 Americans has been a victim of "revenge porn".

Leukfeldt, R. (2017). Research Agenda: The Human Factor in Cybercrime and Cybersecurity. The Hague: Eleven International Publishing.

Leukfeldt, E. R., & Yar, M. (2016). Applying routine activity theory to cybercrime: A theoretical and empirical analysis. Deviant Behavior, 37(3), 263-280, DOI:10.1080/01639625.2015.1012409.

Leukfeldt, E. R., Kleemans, E. R., & Stol, W. P. (2017). Cybercriminal networks, social ties and online forums: social ties versus digital ties within phishing and malware networks. The British Journal of Criminology, 57(3), 704-722, DOI:10.1093/bjc/azw009.

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

Li, X. (2017). A Review of Motivations of Illegal Cyber Activities. Kriminologija & Socijalna Integracija, 25(1), 110-126, DOI:10.31299/ksi.25.1.4.

Lianos, H., & McGrath, A. (2018). Can the general theory of crime and general strain theory explain cyberbullying perpetration? Crime & Delinquency, 64(5), 674-700, DOI:10.1177/0011128717714204.

Liggett, R., Lee, J. R., Roddy, A. L., & Wallin, M. A. (2020). The Dark Web as a Platform for Crime: An Exploration of Illicit Drug, Firearm, CSAM, and Cybercrime Markets. In T. J. Holt, & A. M. Bossler, The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 91-116, DOI:10.1007/978-3-319-78440-3_17). New York: Springer International Publishing AG.

Lupovici, A. (2011). Cyber warfare and deterrence: Trends and challenges in research. *Military and Strategic Affairs*, *3*(3), 49-62.

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

Mahadevan, P. (2020). "A Social Anthropology of Cybercrime. The digitization of India's economic periphery". Retrieved from https://globalinitiative.net/wp content/uploads/2020/04/India-Cybercrime.10.04.web_.pdf

Maimon, D. (2020). Deterrence in Cyberspace: An Interdisciplinary Review of the Empirical Literature. *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, 449-467.

Maiwald, E. (2003). Network Security: A Beginner's Guide (Second Edition ed.). California, USA: McGraw-Hill Osborne Media.

MalwareBytes Labs (2020). 2020 State of Malware Report. Available at: https://www.malwarebytes.com/resources/files/2020/02/2020_state-of-malware-report-1.pdf

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.

Marttila, E., Koivula, A., & Räsänen, P. (2021). Cybercrime Victimization and Problematic Social Media Use: Findings from a Nationally Representative Panel Study. American Journal of Criminal Justice, 46(6), 862-881.

Matza, D. (2009/1964). Delinquency & Drift (Vol. V). New Jersey: Transaction Publishers/John Wiley & Sons.

MacFarlane, L., & Bocij, P. (2003). An exploration of predatory behaviour in cyberspace: Towards a typology of cyberstalkers. First Monday, 8(9).

McGrew, R. (2006, January). Experiences with honeypot systems: Development, deployment, and analysis. In *Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06)* (Vol. 9, pp. 220a-220a). IEEE.

McGuire, M. (2019). *Social Media Platforms and the Cybercrime Economy*. Cambridge: Bromium.

McGuire, M. (2020). It ain't what it is, it's the way that they do it? Why we still don't understand cybercrime. In R. Leukfeldt, & T. J. Holt (Eds.), The Human Factor of Cybercrime (pp. 3-28). New York: Routledge.

McGuire, M. & Dowling, S. (2013). Cyber crime: A review of the evidence Research. Summary of key findings and implications. Home Office Research Report 75, Available at: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/246749/horr75-summary.pdf.

Majumder, A., Routh, M., & Singha, D. (2019). A Conceptual Study on the Emergence of Cryptocurrency Economy and Its Nexus with Terrorism Financing. In The Impact of Global Terrorism on Economic and Political Development. Emerald Publishing Limited.

Mehta, A. (2021, May 21). 'Callous' ransomware attack has caused 'catastrophic' damage to Irish health care system. Retrieved July 31, 2021, from Sky News: https://news.sky.com/story/callous-ransomware-attack-has-caused-catastrophic-damage-to-irish-health-care-system-12312243

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

Merton, R. K. (1968). Social theory and social structure. New York: Free Press.

Mikkola, M. O.-J. (2020). Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context.Situational and Individual Risk Factors for Cybercrime Victimization in a Cross-national Context. International Journal of Offender Therapy and Comparative Criminology.

Moneva, A., Miró-Llinares, F., & Hart, T. C. (2021). Hunter or Prey? Exploring the situational profiles that define repeated online harassment victims and offenders. Deviant Behavior, 42(11), 1366-1381.

Montiel, I., Carbonell, E., & Pereda, N. (2016). Multiple online victimization of Spanish adolescents: Results from a community sample. Child Abuse & Neglect, 52, 123-134.

Mueller-Smith, M., & Schnepel, K. T. (2020). Diversion in the Criminal Justice System. The Review of Economic Studies, rdaa030, DOI:10.1093/restud/rdaa030.

Muggah, R., & Nathan, T. (2015). Brazil's Cybercrime Problem. Foreign Affairs.

Nadim, M., & Fladmoe, A. (2021). Silencing women? Gender and online harassment. *Social Science Computer Review*, 39(2), 245-258.

National centre for Missing and Exploited Children . (2020). CyberTipline 2020: Rise in Online Enticement and Other Trends From Exploitation Stats. Retrieved from National centre for Missing and Exploited Children: https://www.missingkids.org/blog/2021/rise-in-online-enticement-and-other-trends--ncmec-releases-2020-

National Cyber Crime Unit / Prevent Team. (2017, January 13). Pathways Into Cyber Crime. Retrieved from National Crime Agency (NCA): https://www.nationalcrimeagency.gov.uk/who-we-are/publications/6-pathways-into-cyber-crime-1/file

Navarro, Jordana N., Catherine D. Marcum, George E. Higgins and Melissa L. Ricketts (2016). "Addicted to the Thrill of the Virtual Hunt: Examining the Effects of Internet Addiction on the Cyberstalking Behaviors of Juveniles." Deviant Behavior 37 (2016): 893 - 903.

Navarro, J. N., & Marcum, C. D. (2020). Deviant Instruction: The Applicability of Social Learning Theory to Understanding Cybercrime. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 527-545.

Neufeld, D. J. (2010). Understanding Cybercrime. 2010 43rd Hawaii International Conference on System Sciences (pp. 1-10, DOI:10.1109/HICSS.2010.417). IEEE.

Ngejane, C. H., Mabuza-Hocquet, G., Eloff, J. H., & Lefophane, S. (2018). Mitigating online sexual grooming cybercrime on social media using machine learning: A desktop survey.

In 2018 International Conference on Advances in Big Data, Computing and Data Communication Systems (icABCD) (pp. 1-6). IEEE.

Noble, W. (2020). A Nietzschean Analysis of Cybercrime and Deviance (Doctoral dissertation, University of Central Lancashire).

Nurse, J. R. (2018). Cybercrime and you: How criminals attack and the human factors that they seek to exploit. arXiv preprint arXiv:1811.06624.

Nussbaum, B., & Udoh, E. S. (2020). Surveillance, Surveillance Studies, and Cyber Criminality. In T. J. Holt, & A. M. Bossler, The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 156-182). Cham, Switzerland: Springer International Publishing AG.

Nye, J. S. (2017). Deterrence and Dissuasion in Cyberspace. International Security, Vol. 41, No. 3, pp. 44–71.

Oksanen, A., Oksa, R., Savela, N., Kaakinen, M., & Ellonen, N. (2020). Cyberbullying victimization at work: Social media identity bubble approach. Computers in human behavior, 109, 106363.

Oliver, J., Cheng, S., Manly, L., Zhu, J., Paz, R. D., Sioting, S., & Leopando, J. (2012). Blackhole Exploit Kit: A Spam Campaign. *Not a Series of Individual Spam Runs*, *10*, 17.

Olofinbiyi, S. A. (2021). Exploring Youth Awareness of Cybercrime and Factors Engendering its Proliferation in Nigeria. *African Renaissance*, 18(4), 319.

Owenson, G. H., & Savage, N. J. (2015). The tor dark net. (Global Commission on Internet Governance; No. 20). Centre for International Governance Innovation. https://www.cigionline.org/publications/tor-dark-net

Paoli, L., Visschers, J., Verstraete, C., & Van Hellemont, E. (2018). *The Impact of Cybercrime on Belgian Businesses.* Intersentia.

Parsons, C., Molnar, A., Dalek, J., Knockel, J., Kenyon, M., Haselton, B., . . . Deibert, R. (2019). The Predator in Your Pocket: A Multidisciplinary Assessment of the Stalkerware Application Industry. Toronto: Citizen Lab.

Pastrana, S., Thomas, D. R., Hutchings, A., & Clayton, R. (2018). Crimebb: Enabling cybercrime research on underground forums at scale. Proceedings of the 2018 World Wide Web Conference (pp. 1845-1854). Lyon: International World Wide Web Conferences Steering Committee Republic and Canton of Geneva Switzerland.

Paulhus, D. L., & Williams, K. M. (2002). The dark triad of personality: Narcissism, Machiavellianism, and psychopathy. Journal of research in personality, 36(6), 556-563, DOI:10.1016/S0092-6566(02)00505-6.

Payne, B. K. (2020). Defining Cybercrime. In T. J. Holt, & A. M. Bossler, The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 3-25, DOI: 10.1007/978-3-319-78440-3_1 3). New York: Springer International Publishing AG.

Payne, B. K., Hawkins, B., & Xin, C. (2019a). Using labeling theory as a guide to examine the patterns, characteristics, and sanctions given to cybercrimes. American Journal of Criminal Justice, 44(2), 230-247, DOI:10.1007/s12103-018-9457-3.

Payne, B., May, D. C., & Hadzhidimova, L. (2019b). America's most wanted criminals: Comparing cybercriminals and traditional criminals. Criminal Justice Studies, 32(1), 1-15, DOI:10.1080/1478601X.2018.1532420.

Phillips, K., Davidson, J., Farr, R., Burkhardt, C., Caneppele, S., & Aiken, M. (2021). Conceptualising Cybercrime: Definitions, Typologies and Taxonomies. Manuscript submitted for publication.

Pihelgas, M. (2013). Back-Tracing and Anonymity in Cyberspace. In K. Ziolkowski, Peacetime Regime for State Activities in Cyberspace. International Law, International Relations and Diplomacy (pp. 31-60). Tallinn: NATO Cooperative Cyber Defence Centre of Excellence.

Plotnek, J. J., & Slay, J. (2021). Cyber terrorism: A homogenized taxonomy and definition. Computers & Security, 102, 102145.

Pollock, E. (2009). Researching white supremacists online: methodological concerns of researching hate 'speech'. Internet Journal of Criminology, 1-19.

Portnoff, R. S., Huang, D. Y., Doerfler, P., Afroz, S., & McCoy, D. (2017, August). Backpage and bitcoin: Uncovering human traffickers. In *Proceedings of the 23rd ACM SIGKDD International Conference on Knowledge Discovery and Data Mining* (pp. 1595-1604).

Powell, A., Henry, N., Flynn, A., & Scott, A. J. (2018). Image-based sexual abuse: The extent, nature, and predictors of perpetration in a community sample of Australian residents. *Computers in Human Behavior*, *92*, 393-402.

Pratt, T. C., & Turanovic, J. J. (2016). Lifestyle and routine activity theories revisited: The importance of "risk" to the study of victimization. Victims & Offenders, 11(3), 335-354.

Psilakis, A. (2019). Cybercrime. *IELR*, 35, 195.

Rhodes, L. M. (2017). Human trafficking as cybercrime. *AGORA International Journal of Administration Sciences*, 1(1), 23-29.

Riva, G., Mantovani, F., Capideville, C. S., Preziosa, A., Morganti, F., Villani, D., . . . Alcañiz, M. (2007). Affective interactions using virtual reality: the link between presence and emotions. CyberPsychology & Behavior, 10(1), 45-56, DOI:10.1089/cpb.2006.9993.

Rogers, M. K., Siegfried, K., & Tidke, K. (2006). Self-reported computer criminal behaviour: A psychological analysis. Digital Investigation, 3, S116–S120, DOI: 10.1016/j.diin.2006.06.002.

Ronggong, H., & Lijia, J. (2020). Preventive cybercrime and cybercrime by omission in China. In *Artificial Intelligence and the Law* (pp. 74-96). Routledge.

Rosenzweig, M. R. (2002). Biological psychology: An introduction to behavioral, cognitive, and clinical neuroscience (3rd edition ed.). Washington: American Psychological Association.

Roundy, K. A., Mendelberg, P. B., Dell, N., McCoy, D., Nissani, D., Ristenpart, T., & Tamersoy, A. (2020). The many kinds of creepware used for interpersonal attacks. 2020 IEEE Symposium on Security and Privacy (SP) (pp. 626-643). IEEE.

Ruvalcaba, Y., & Eaton, A. A. (2020). Nonconsensual pornography among US adults: a sexual scripts framework on victimization, perpetration, and health correlates for women and men. Psychology of violence, 10(1), 68.

Sabillon, R., Cavaller, V., Cano, J., & Serra-Ruiz, J. (2016, June). Cybercriminals, cyberattacks and cybercrime. In *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)* (pp. 1-9). IEEE.

De Santisteban, P., Del Hoyo, J., Alcázar-Córcoles, M. Á., & Gámez-Guadix, M. (2018). Progression, maintenance, and feedback of online child sexual grooming: A qualitative analysis of online predators. Child Abuse & Neglect, 80, 203-215.

Salter, M., Wong, W. T., Breckenridge, J., Scott, S., Cooper, S., & Peleg, N. (2021). Production and distribution of child sexual abuse material by parental figures. Trends and Issues in Crime and Criminal Justice, (616), 1-17.

Sarre, R., Lau, L. Y.-C., & Chang, L. Y. (2018). Responding to cybercrime: current trends. *Police Practice and Research*, *19*(6), 515-518.

Schell, B. (2020). Internet Addiction and Cybercrime. In T. J. Holt, & A. M. Bossler, The Palgrave Handbook of International Cybercrime and Cyberdeviance (pp. 679-703, DOI:10.1007/978-3-319-78440-3). Cham, Switzerland: Palgrave Macmillan, Cham.

Schreuders, C. (2019). Understanding Cybercrime Victimisation: Modelling the Local Area Variations in Routinely Collected Cybercrime Police Data Using Latent Class Analysis. *International Journal of Cyber Criminology*, 13(2), 493-510.

Schreuders, Z. C. (2018). Characteristics of Victims of Cybercrime.

Scrivens, R., Gill, P., & Conway, M. (2020). The role of the internet in facilitating violent extremism and terrorism: suggestions for progressing research. The Palgrave Handbook of International Cybercrime and Cyberdeviance, 1417-1435.

Scroxton, A. (2021). Hacked Finnish therapy business collapses. Retrieved 2021, from www.computerweekly.com: https://www.computerweekly.com/news/252496227/Hacked-Finnish-therapy-business-collapses

Smith, G.S. (2015), "Management models for international cybercrime", *Journal of Financial Crime*, Vol. 22 No. 1, pp. 104-125.

Soudijn, M.R.J., Zegers B.C.H.T. (2012) Cybercrime and virtual offender convergence settings. Trends Organ Crim 15, 111–129 https://doi.org/10.1007/s12117-012-9159-z

Seigfried-Spellar, K. C., Villacís-Vukadinović, N., & Lynam, D. R. (2017). Computer criminal behavior is related to psychopathy and other antisocial behavior. Journal of Criminal Justice, 51, 67-73.

Selzer, N., & Oelrich, S. (2021). Saint or Satan? Moral Development and Dark Triad Influences on Cybercriminal Intent.

Soska, K., & Christin, N. (2015). Measuring the Longitudinal Evolution of the Online Anonymous Marketplace Ecosystem. *USENIX Security Symposium*.

Soomro, T. R., & Hussain, M. (2019). Social Media-Related Cybercrimes and Techniques for Their Prevention. Appl. Comput. Syst., 24(1), 9-17.

Speckhard, A., & Ellenberg, M. (2020). Is internet recruitment enough to seduce a vulnerable individual into terrorism. Homeland Security Today.

Strawhun J, Adams N, Huss MT (2013). The assessment of cyberstalking: an expanded examination including social networking, attachment, jealousy, and anger in relation to violence and abuse. Violence Vict. 2013;28(4):715-30.

Suler, J. (2004). The Online Disinhibition Effect. Cyberpsychology & behavior , 7(3), 321-326, DOI: 10.1089/1094931041291295.

Symantec (2019). ISTR Internet Security Threat Report Volume 24. Available at: https://docs.broadcom.com/doc/istr-24-2019-en

Takatalo, J., Nyman, G., & Laaksonen, L. (2008). Components of human experience in virtual environments. Computers in Human Behavior, 24(1), 1-15, DOI: 10.1016/j.chb.2006.11.003.

Tambe, A., Aung, Y. L., Sridharan, R., Ochoa, M., Tippenhauer, N. O., Shabtai, A., & Elovici, Y. (2019, March). Detection of threats to IoT devices using scalable VPN-forwarded

honeypots. In *Proceedings of the Ninth ACM Conference on Data and Application Security and Privacy* (pp. 85-96).

Tasnim, S., Hossain, M. M., & Mazumder, H. (2020). Impact of rumors and misinformation on CO- VID-19 in social media. *Journal of Preventive Medicine and Public Health*, *53*(3), 171–174. doi:10.3961/ jpmph.20.094 PMID:32498140

Teichmann, F. M. J. (2018). Financing terrorism through cryptocurrencies–a danger for Europe?. Journal of Money Laundering Control.

Tennakoon, H. (2011). The need for a comprehensive methodology for profiling cyber-criminals. Retrieved from new Security Learning : http://www.newsecuritylearning.com/index.php/archive/150-the-need-for-a-comprehensive-methodology-for-profiling-cyber-criminals

Terwilliger, A. M. (2021). The Role of Social Media in Human Trafficking Victimization (Doctoral dissertation, Nova Southeastern University).

Thomas, D., & Loader, B. (2000). Cybercrime: Law enforcement, security and surveillance in the information age. (D. Thomas, & B. Loader, Eds.) London: Routledge.

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

Turvey, B. E. (2012). *A History of Criminal Profiling.* Oxford: Academic Press.

Ullrich, S., Borkenau, P., & Marneros, A. (2001). Personality disorders in offenders: Categorical versus dimensional approaches. Journal of Personality Disorders, 15(5), 442-449.

UNDOC. (2010, August). Handbook on the Crime Prevention Guidelines: Making them work. Criminal Justice Handbook Series, pp. https://www.unodc.org/pdf/criminal_justice/Handbook_on_Crime_Prevention_Guidelines_-_Making_them_work.pdf.

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

Vold, G. B. (1958). Theoretical criminology.

Wachs, S., Wolf, K. D., & Pan, C. C. (2012). Cybergrooming: Risk factors, coping strategies and associations with cyberbullying. Psicothema, 628-633.

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.

Wall, D. (2017). Crime, security and information communication technologies: The changing cybersecurity threat landscape and implications for regulation and policing. In B. R, S. E, & Y. K, The Oxford Handbook on the Law and Regulation of Technology (pp. 1075–1096). Oxford: Oxford University Press.

Walrave, M., Heirman, W., & Hallam, L. (2014). Under pressure to sext? Applying the theory of planned behaviour to adolescent sexting. Behaviour & Information Technology, 33(1), 86-98, DOI:10.1080/0144929X.2013.837099.

Warren, M., & Leitch, S. (2009). Hacker Taggers: A new type of hackers. Information Systems Frontiers, 12(4), 425-431, DOI:10.1007/s10796-009-9203-y.

Westlake, B. G. (2020). The past, present, and future of online child sexual exploitation: Summarizing the evolution of production, distribution, and detection. *The Palgrave handbook of international cybercrime and cyberdeviance*, 1225-1253.

Weimann, G. (2005). Cyberterrorism: The sum of all fears?. Studies in Conflict & Terrorism, 28(2), 129-149.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013). A review of online grooming: Characteristics and concerns. Aggression and violent behavior, 18(1), 62-70.

Whittle, H., Hamilton-Giachritsis, C., Beech, A., & Collings, G. (2013b). A review of young people's vulnerabilities to online grooming. Aggression and violent behavior, 18(1), 135-146.

Whitty, M. T. (2018). Do you love me? Psychological characteristics of romance scam victims. Cyberpsychology, behavior, and social networking, 21(2), 105-109.

Whitty, M. T. (2019). Who can spot an online romance scam?. Journal of Financial Crime.

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

Wilsem, J. V. (2013). Hacking and harassment—Do they have something in common? Comparing risk factors for online victimization. Journal of Contemporary Criminal Justice, 29(4), 437-453.

Wittes, B., Poplin, C., Jurecic, Q., & Spera, C. (2016). Closing the sextortion sentencing gap: a legislative proposal. Center for Technology Innovation at Brookings. https://www. brookings. edu/research/closing-the-sextortion-sentencing-gap-a-legislative-proposal/. Accessed, 16.

Wolak, J., Finkelhor, D., & Mitchell, K. J. (2012). Trends in Law Enforcement Responses to Technology-facilitated Child Sexual Exploitation Crimes: TheThird National Juvenile OnlineVictimization Study (NJOV-3).

Wolak, J., Finkelhor, D., Walsh, W., & Treitman, L. (2018). Sextortion of minors: Characteristics and dynamics. Journal of Adolescent Health, 62(1), 72-79.

World Health Organisation. (2021a, February 3). *WHO publishes public health research agenda for managing infodemics.* WHO. https://www.who.int/publications/i/item/9789240019508

World Health Organisation. (2021b). *World Health Organisation Newsroom*. WHO. https://www.who. int/news-room/spotlight/let-s-flatten-the-infodemic-curve

Wybo, J. L., Fogelman-Soulié, F., Gouttas, C., Freyssinet, É., & Lions, P. (2015). Impact of social media in security and crisis management: a review. International Journal of Emergency Management, 11(2), 105-128.

Yao, Mike & Linz, Daniel. (2008). Predicting Self-Protections of Online Privacy. Cyberpsychology & behavior: the impact of the Internet, multimedia and virtual reality on behavior and society. 11. 615-7. 10.1089/cpb.2007.0208.

Young, S., Greer, B., & Church, R. (2017). Juvenile delinquency, welfare, justice and therapeutic interventions: a global perspective. BJPsych Bulletin, 41, 21-29, DOI:10.1192/pb.bp.115.052274.

Younies, Hassan, and Tareq Na. "Effect of cybercrime laws on protecting citizens and businesses in the United Arab Emirates (UAE)." Journal of Financial Crime (2020).

Zaleski, K. L., Gundersen, K. K., Baes, J., Estupinian, E., & Vergara, A. (2016). Exploring rape culture in social media forums. Computers in Human Behavior, 63, 922-927.

Zhou, G., Zhuge, J., Fan, Y., Du, K., & Lu, S. (2020). A market in dream: the rapid development of anonymous cybercrime. *Mobile Networks and Applications*, 25(1), 259-270.