EUROPOL

INTERNET ORGANISED CRIME THREAT ASSESSMENT

2020

IOCTA
[2020]

get.password+

launch.attack

EUROPOL

INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA) 2020

www.europol.europa.eu

Contents

Foreword

Catherine De Bolle
Executive Director of Europol

I am pleased to introduce the Internet Organised Crime Threat Assessment (IOCTA) 2020.

The IOCTA is Europol's flagship strategic product highlighting the dynamic and evolving threats from cybercrime. It provides a unique law enforcement-focused assessment of emerging challenges and key developments in the area of cybercrime. We are grateful for the many contributions from our colleagues within European law enforcement community and to our partners in the private industry for their input to the report. Combining law enforcement and private sector insights allows us to present this comprehensive overview of the threat landscape.

The data collection for the IOCTA 2020 took place during the lockdown implemented as a result of the COVID-19 pandemic. Indeed, the pandemic prompted significant change and criminal innovation in the area of cybercrime. Criminals devised both new modi operandi and adapted existing ones to exploit the situation, new attack vectors and new groups of victims.

The analysis for the IOCTA 2020 clearly highlights cybercrime as a fundamental feature of the European crime landscape. Cybercrime remains among the most dynamic forms of crime encountered by law enforcement in the EU. While ransomware, business email compromise and social engineering are familiar cybercrime threats, their execution evolves constantly and makes these criminal activities more complex to detect and to investigate. Ransomware in particular remains a priority threat encountered by cyber investigators across the EU. The amount of online child sexual abuse material detected continues to increase, further exacerbated by the COVID-19 pandemic, which has had serious consequences for the investigative capacity of law enforcement authorities.

Europol is at the forefront of law enforcement innovation and offers various policing solutions in relation to encryption, cryptocurrencies and other challenges. The European Cybercrime Centre (EC3) at Europol is the platform of choice for cybercrime investigators across the EU and beyond to connect, collaborate and communicate.

The case studies illustrating this report demonstrate the necessity and effectiveness of international law enforcement cooperation in tackling cybercrime as well as the vital role played by private-public partnerships in this area. Europol provides an ideal framework for these different stakeholders to come together, exchange information and take concerted action.

Cybercrime affects citizens, businesses and organisations across the EU. Europol plays a key role in countering cybercrime by working with our many partners in law enforcement and the private sector and by offering innovative solutions and effective, comprehensive support to investigations. I hope this analysis can inform effective responses to these evolving threats and make Europe safer.

Abbreviations

AaaS Access-as-a-Service

AI Artificial Intelligence

ATM Automated teller machine

BEC Business email compromise

BPH Bulletproof hosting

CaaS Cybercrime-as-a-Service

C&C Command & control

CNP Card-not-present

CSAM Child sexual abuse material

CSE Child sexual exploitation

DDoS Distributed Denial of Service

DNS Domain Name System

DoH DNS over HTTPs

E-commerce Electronic commerce

EC3 Europol's European Cybercrime Centre

E-skimming Electronic skimming

GDPR General Data Protection Regulation

HTML Hypertext Markup Language

HTTP Hypertext Transfer Protocol

HTTPs Hypertext Transfer Protocol Secure

IOCTA Internet Organised Crime Threat Assessment

IoT Internet of Things

IP Internet protocol

ISP Internet service provider

IT Information technology

J-CAT Joint Cybercrime Action Taskforce

KYC Know your customer

LDCA Live distant child abuse

MaaS Malware-as-a-Service

NCMEC The National Center for Missing and Exploited Children

OTP One time password

PC Personal computer

PGP Pretty Good Privacy

POS Point of sale

P2P Peer-to-peer

RaaS Ransomware-as-a-Service

RATs Remote access tools

RDP Remote desktop protocol

SIM Subscriber identity module

SQL Structured query language

Tor The onion router

VIDTF Victim Identification Taskforce

VPN Virtual private network

VPS Virtual private server

2FA Two-factor authentication

Executive summary

The threat landscape over the last year described in the IOCTA 2020 contains many familiar main characters. The starring roles in terms of priority threats went to the likes of social engineering, ransomware and other forms of malware. Several interviewees captured the essence of the current state of affairs of the threat landscape by stating: cybercrime is an evolution, not a revolution. As time passes, the cyber-element of cybercrime infiltrates nearly every area of criminal activity. Key elements mentioned in previous editions of the IOCTA that return this year merit more, rather than less, attention. The repetition means the challenge still exists and has, in many cases, increased, underlining the need to further strengthen the resilience and response to well-known threats. The IOCTA 2020 makes clear that the fundamentals of cybercrime are firmly rooted, but that does not mean cybercrime stands still. Its evolution becomes apparent on closer inspection, in the ways seasoned cybercriminals refine their methods and make their artisanship accessible to others through crime as a service.

The COVID-19 crisis illustrated how criminals actively take advantage of society at its most vulnerable. Criminals tweaked existing forms of cybercrime to fit the pandemic narrative, abused the uncertainty of the situation and the public's need for reliable information. Across the board from social engineering to Distributed Denial of Service (DDoS) attacks and from ransomware to the distribution of child sexual abuse material (CSAM), criminals abused the crisis when the rest of society was trying to contain the situation. The opportunistic behaviour of criminals during the pandemic, however, should not overshadow the overall threat landscape. In many cases, COVID-19 caused an amplification of existing problems exacerbated by a significant increase in the number of people working from home. This is perhaps most noticeable in the area of child sexual abuse and exploitation. As in previous years, the amount of online CSAM detected continues to increase, further exacerbated by the COVID-19 crisis, which has had serious consequences for the investigative capacity of law enforcement authorities. In addition, livestreaming of child sexual abuse increased and became even more popular during the COVID-19 crisis; a recent case shows production also takes place in the EU.

Data compromise once more features as a central aspect throughout a number of threats. Both law enforcement and private sector representatives consistently report on social engineering among the top threats. With regard to social engineering, in particular phishing, cybercriminals are now employing a more holistic strategy by demonstrating a high level of competency when exploiting tools, systems and vulnerabilities, assuming false identities and working in close cooperation with other cybercriminals. However, despite the trend pointing towards a growing sophistication of some criminals, the majority of social engineering and phishing attacks are successful due to inadequate security measures or insufficient awareness of users. In particular, as attacks do not have to be necessarily refined to be successful.

The developments in the area of non-cash payment fraud over the past twelve months reflect the overall increase in sophistication and targeting of social engineering and phishing. Fuelled by a wealth of readily available data, as well as a Cybercrime-as-a-Service (CaaS) community, it has become easier for criminals to carry out highly targeted attacks. As a result, law enforcement and industry continue to identify well-established frauds as a major threat.

Subscriber identity module (SIM) swapping is one of the new key trends this year, having caused significant losses and attracted considerable attention from law enforcement. As a highly targeted type of social engineering attack, SIM swapping can have potentially devastating consequences for its victims, by allowing criminals to bypass text message-based (SMS) two-factor authentication (2FA) measures gaining full control over their victims' sensitive accounts.

Business Email Compromise (BEC) continues to increase. As criminals are more carefully selecting their targets, they have shown a significant understanding of internal business processes and systems' vulnerabilities. At the same time, certain other forms of fraud have entered the spotlight due to the sheer number of victims they have generated.

The spread of online investment fraud all over Europe is not necessarily new but has generated increased law enforcement attention as victims at times lose their life savings to professional organised criminal groups that have incorporated cyber elements into their scams.

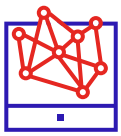
The clear majority of law enforcement respondents once again named ransomware as a top priority threat. Although this point has been made in past editions of the IOCTA, ransomware remains one of the, if not the, most dominant threats, especially for public and private organisations within as well as outside Europe. Considering the scale of damage that ransomware can inflict, victims also appear to be reluctant to come forward to law enforcement authorities or the public when they have been victimised, which makes it more difficult to identify and investigate such cases. Criminals continued making their ransomware attacks increasingly targeted. Ransomware has shown to pose a significant indirect threat to businesses and organisations, including in critical infrastructure, by targeting supply chains and third-party service providers. Perhaps one of the most crucial developments is the new way of pressuring victims to pay by stealing and subsequently threatening to auction off victims' sensitive data.

Besides ransomware, European law enforcement reported malware in the broader sense to be widely present in cybercrime cases. Criminals have converted some traditional banking Trojans into more advanced modular malware to cover a broader scope of functionality. These evolved forms of modular malware are a top threat in the EU, especially as their adaptive and expandable nature makes them increasingly more complicated to combat effectively.

With a range of threat actors, this makes drawing general conclusions about particular threats challenging. In areas ranging from social engineering and phishing, to ransomware and other forms of malware, law enforcement authorities witness a broad spectrum of threat actors. These actors vary in terms of level of skill, capability and adaptability. The top tier criminals manage to run their operations like a professional enterprise, whereas less sophisticated threat actors tend to rely on off-the-shelf materials to conduct their criminal activities. The availability of the materials through CaaS, however, continues to make such activities accessible. Moreover, across the board threat actors in different types of cybercrime demonstrate their resilience. Perhaps more importantly, in areas such as the Darkweb, criminals have enhanced their cooperation and joined forces to provide a response to shared challenges. This means they are able to make their business more robust and in particular incorporate better security solutions to ensure that law enforcement are unable to trace them. Overall, cybercriminals are showing an improved level of operational security and proving to be highly aware of how to hide their identities and criminal activities from law enforcement or private sector companies. With cryptocurrencies, criminals also manage to complicate law enforcement's ability to trace payments connected to criminal activities.

To respond to the cybercrime challenges in a more effective manner, a number of key ingredients are essential. First, information sharing is at the heart of any strategic, tactical and operational response regardless of the specific type of cybercrime. Sharing information, which needs to be purpose-driven and actionable, requires reliable coordination and cooperation from public and private partners. At the same time, information sharing requires a legal framework and attitude that is sensitive to the timely exchange of information, which is crucial as cybercriminals can move their infrastructure within the blink of an eye. This is particularly evident in the criminal abuse of the Darkweb, where short lifecycles of marketplaces influences law enforcement's ability to conduct investigations. There is also the need to foster a culture of acceptance and transparency when organisations or individuals fall victim to cybercrime. Re-victimising victims after a cyber-attack is counterproductive and a significant challenge, as law enforcement need companies and individuals who have been subject of a crime to come forward. This can help resolve the challenges in reporting we currently face. Besides information sharing through enhanced coordination and cooperation, other key elements to include in an effective response are prevention and awareness and capacity building. We can reduce the success rate of many forms of cybercrime by educating individuals and organisations in recognising criminal activity before they fall victim to it. It is worth underlining the importance of the responsibility of industry in integrating security and privacy in their design as fundamental principles, instead of shaming end users as the weakest link. Through capacity building, on the other hand, law enforcement across different crime areas will be able to understand and respond to the cyber-element of crimes. Finally, taskforce work such as coordinating and de-conflicting law enforcement operational response, for which the Europol Joint Cybercrime Action Taskforce (J-CAT) platform is vital, continues to play a key role in the current cybercrime landscape.

Key findings



CROSS-CUTTING CRIME FACILITATORS AND CHALLENGES TO CRIMINAL INVESTIGATIONS

- Social engineering remains a top threat to facilitate other types of cybercrime.
- Cryptocurrencies continue to facilitate payments for various forms of cybercrime, as developments evolve with respect to privacy-oriented crypto coins and services.
- Challenges with reporting hinder the ability to create an accurate overview of crime prevalence across the EU.

CYBER-DEPENDENT CRIME

- Ransomware remains the most dominant threat as criminals increase pressure by threatening publication of data if victims do not pay.
- Ransomware on third-party providers also creates potential significant damage for other organisations in the supply chain and critical infrastructure.
- Emotet is omnipresent given its versatile use and leads the way as the benchmark of modern malware.
- The threat potential of DDoS attacks is higher than its current impact in the EU.

CHILD SEXUAL EXPLOITATION ONLINE

- The amount of online CSAM detected continues to increase, further exacerbated by the COVID-19 crisis, which has serious consequences for the capacity of law enforcement authorities.
- The use of encrypted chat apps and industry proposals to expand this market pose a substantial risk for abuse and make it more difficult for law enforcement to detect and investigate online CSE activities.
- Online offender communities exhibit considerable resilience and are continuously evolving.
- Livestreaming of child sexual abuse continues to increase and became even more prevalent during the COVID-19 crisis.
- The commercialisation of online CSE is becoming a more widespread issue, with individuals uploading material to hosting sites and subsequently acquiring credit on the basis of the number of downloads.

PAYMENT FRAUD

- SIM swapping is a key trend that allows perpetrators to take over accounts and has demonstrated a steep rise over the last year.
- BEC remains an area of concern as it has increased, grown in sophistication, and become more targeted.
- Online investment fraud is one of the fastest growing crimes, generating millions in losses and affecting thousands of victims.
- Card-not-present (CNP) fraud continues to increase as criminals diversify in terms of target sectors and electronic skimming (e-skimming) modi operandi.

THE CRIMINAL ABUSE OF THE DARKWEB

- The Darkweb environment has remained volatile, lifecycles of Darkweb market places have shortened, and no clear dominant market has risen over the past year compared to previous years to fill the vacuum left by the takedowns in 2019.
- The nature of the Darkweb community at administrator-level shows how adaptive it is under challenging times, including more effective cooperation in the search for better security solutions and safe Darkweb interaction.
- There has been an increase in the use of privacy-enhanced cryptocurrencies and an emergence of privacy-enhanced coinjoin concepts, such as Wasabi and Samurai.
- Surface web e-commerce sites and encrypted communication platforms offer an additional dimension to Darkweb trading to enhance the overall business model.

Introduction

Aim

The IOCTA aims to inform decision-makers at strategic, tactical and operational levels about the threats of cybercrime. The 2020 IOCTA contributes to setting priorities for the 2021 EMPACT operational action plans, which follow the three current priorities defined as:

1) disrupting criminal activities related to attacks against information systems, particularly those following CaaS business models and working as enablers for online crime;

2) combating child sexual abuse and child sexual exploitation, including the production and dissemination of child abuse material;

3) targeting criminals involved in fraud and counterfeiting of non-cash means of payment, including large-scale payment card fraud (especially card-not-present (CNP) fraud), emerging threats to other non-cash means of payment and enabling criminal activities. Furthermore, the IOCTA aims to consolidate findings on current cyber threats, which could contribute to the discussion of research and development priorities as well as planning at the EU-level.

Scope

The scope of the 2020 IOCTA lies in the threat assessment of the cybercrime landscape, consisting of trends and developments pertinent to the EMPACT priorities mentioned previously. In addition to this, the report will discuss other cross-cutting facilitators and challenges that influence or impact the cybercrime ecosystem, such as criminal abuse of cryptocurrencies and social engineering. This report provides an update on the latest trends and the current impact of cybercrime within the EU and beyond.

Methodological approach

For this year's IOCTA, Europol introduced a different methodological approach to gather data. For previous editions, the team shared a survey with all the Member States and several third-party countries. Each crime priority area received a survey, namely cyber-dependent crime, payment fraud, and child sexual exploitation (CSE). This year, as a means to gather more qualitative and in-depth information, the team conducted interviews with representatives from the Member States and Europol partner countries. The team also conducted interviews with Europol experts from the European Cybercrime Centre (EC3) and members of EC3's three advisory groups on internet security, financial services and telecommunication providers.

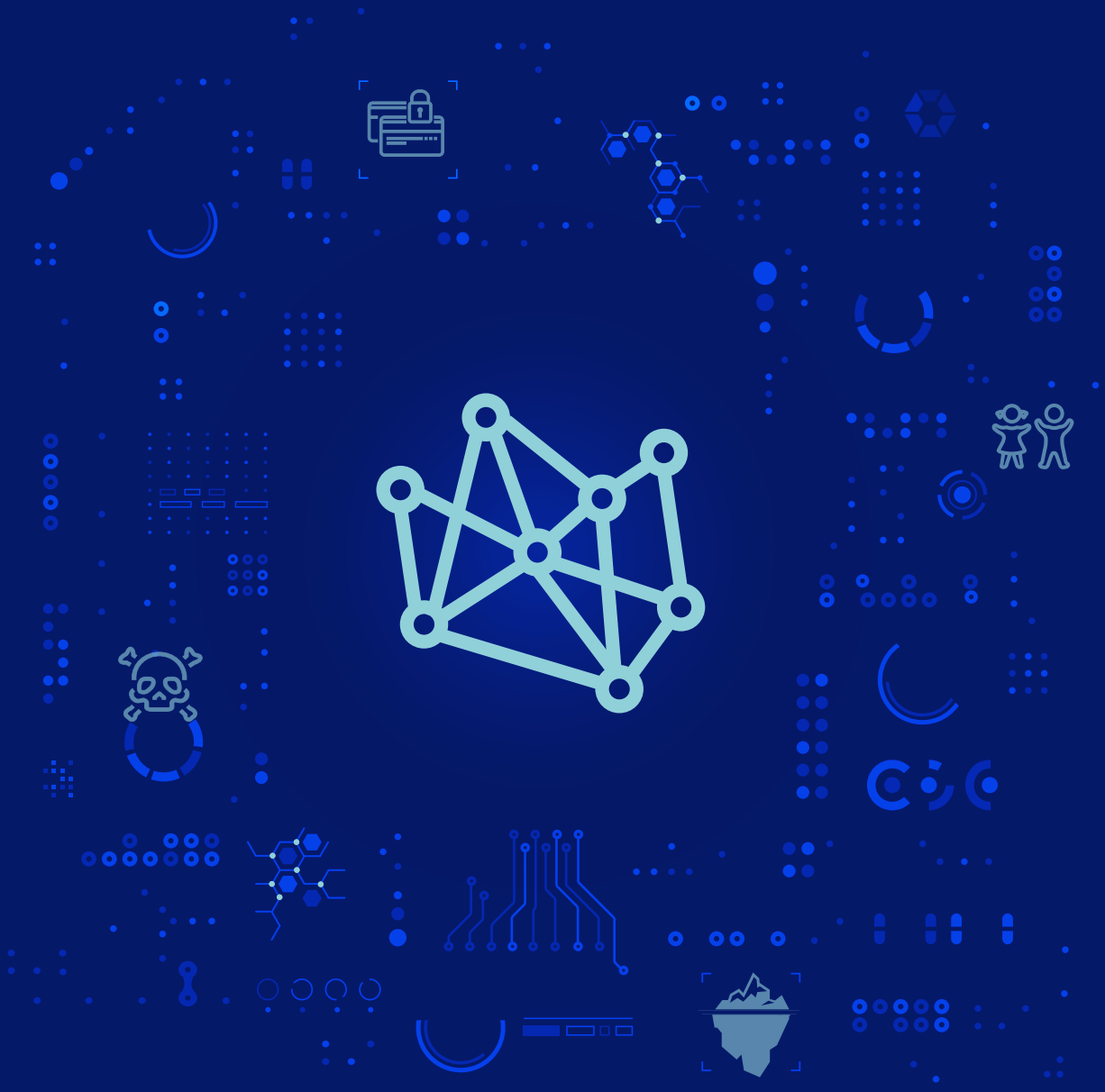
The semi-structured interviews contained open questions. As a result, the range of answers was broader than in the previous structured survey approach wherein which respondents mainly selected from a drop down menu. Through using open questions, answers became less comparable in a traditional sense, but rather than a limitation, the team perceived this is an opportunity to illustrate the complexity of cybercrime especially in connection to establishing a comprehensive threat assessment. The ultimate purpose of the IOCTA is to assist Member States in establishing priorities with respect to cybercrime. This pertains to the type of threats but also concerns other considerations such as how we approach this crime area in terms of analysis.

Cybercrime is inherently complex for a number of reasons. With different perpetrators, different motives, different targets, varying modi operandi, different jurisdictions, etc. there are many variables, which complicate both the ability to gather data as well as the ability to compare findings. Furthermore, the quality of those findings encounter challenges as a result of the ability to register them accurately. These limitations must be taken into consideration with respect to any threat landscape report.

Acknowledgements

Europol would like to extend thanks to all law enforcement and private sector partners who contributed to this report.

1 Cross-cutting crime facilitators and challenges to criminal investigations



KEY FINDINGS

- Social engineering remains an effective top threat to enable other types of cybercrime.
- Cryptocurrencies continue to facilitate payments for various forms of cybercrime, as developments evolve with respect to privacy oriented crypto coins and services.
- Challenges with reporting torment ability to create an accurate overview of crime prevalence across the European Union.

1.1 INTRODUCTION

Throughout the interviews, one message was clear: cybercrime is an evolution not a revolution[1]. The fundamentals of cybercrime stay the same, in that cybercrime is not that much different to other forms of more traditional crime.

This is a crucial observation to include in any assessment, especially as the emphasis when discussing cybercrime is often placed on how quickly cybercrime and, in particular, cybercriminals change their tactics. Perpetrators may operate at the speed of the internet, as they are able to quickly move parts of their infrastructure, alter a particular aspect of the code, adapt the functionality, gather more victim data, etc, but these changes do not inherently alter the threat, especially not at an abstract level at which we discuss the threats within the IOCTA. We can also witness the evolution of cybercrime through the integration of the cyber-component into nearly all forms of traditional crime.

Another reason to reflect on this observation is to understand that to combat cybercrime effectively we need to respond to several challenges. Some of these are included within this chapter of the report, whereas others are included within the respective chapters of the different crime areas. Several of these challenges pertain to the ability of law enforcement to execute its core mission of preventing and combatting crime, identifying suspects, protecting victims and arresting perpetrators.

This chapter contains three key components. First, a reflection on overarching threats that are cross-cutting facilitators for other forms of cybercrime. The second part includes a brief description of a general challenge with respect to gathering (accurate) data about the prevalence of specific forms of cybercrime. The third and final part focuses on challenges which pertain to law enforcement agencies' ability to conduct criminal investigations due to societal developments that criminals opportunistically manage to exploit.

1.2 COVID-19 DEMONSTRATES CRIMINAL OPPORTUNISM

While discussions and models have emerged over several decades surrounding the threats posed by a pandemic crisis, the outbreak of COVID-19 has demonstrated the unfortunate impact potential of such crises on our daily lives across the globe. As physical lockdowns became the norm, cybercrime became more popular than before. There is no denying that the arrival of COVID-19 was a crucial factor in any development discussed with respect to 2020. However, COVID-19 in connection to cybercrime needs to be placed within its context. If anything, COVID-19 demonstrated how cybercrime – at its core – remains largely the same but criminals change the narrative. They adapt the specifics of their approach to fit the societal context as a means to enhance their rate of success. This is not new, in many ways this is business as usual. The difference with COVID-19 is that due to the physical restrictions enacted to halt the spread of the virus, with a subsequent increase in working from home and remote access to business resources, many individuals and businesses that may not have been as active online before the crisis became a lucrative target.

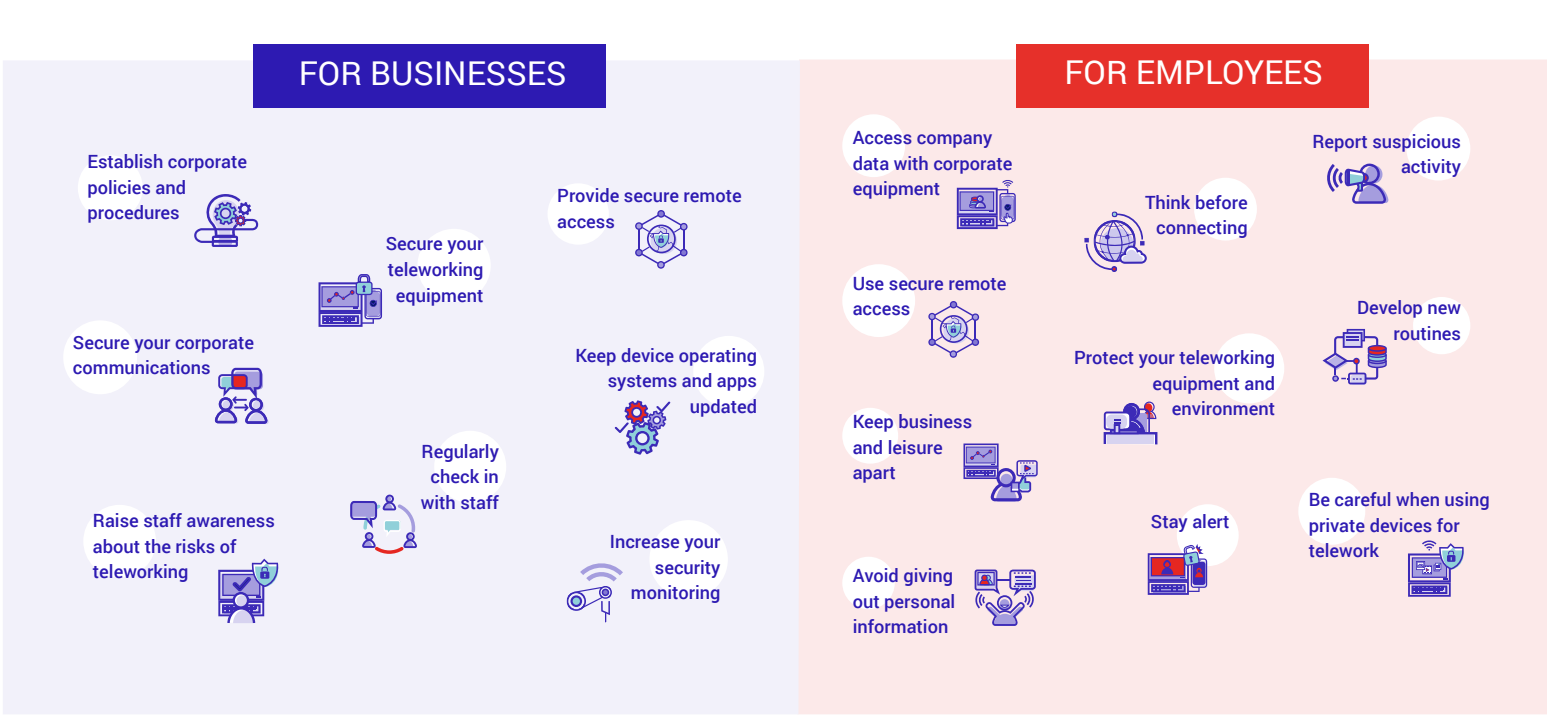
Traditional cybercrime activities such as phishing and cyber-enabled scams quickly exploited the societal vulnerability as many citizens and business were looking for information, answers and sources of help during this time. There were even more challenges for both individuals and business as teleworking during the pandemic became the norm. Europol followed all developments closely and shared its findings through frequent *corona strategic reports*[2].

Spread of disinformation enhances cybercrime opportunities

The pandemic also gave rise to disinformation campaigns and activities. Disinformation efforts are often associated with hybrid threats, which are defined as threats combining conventional and unconventional, military and non-military activities which may be used by non-state or state actors to achieve political aims[3]. A wide range of measures applied in hybrid campaigns include cyber-attacks and disinformation, disruption of critical services, undermining of public trust in governmental institutions and exploiting social vulnerabilities. The presence of disinformation became a crucial feature in the overall threat landscape during the crisis. Many Member States reported problems with respect to the spread of disinformation.

Users become vulnerable and receptive to disinformation and fake news due to the paradoxical oversaturation with available information combined with a perceived lack of trustworthy sources of news that reinforce some of the users' preconceived notions and beliefs. Disinformation can also be linked to cybercrime in efforts to make social engineering and phishing attacks more impactful.

Both seasoned cybercriminals and opportunistic individuals spread disinformation to benefit from it in different ways. Significant political motives can drive disinformation to influence elections or referendums affecting entire countries. However, for criminals the



ultimate aim is always to obtain profit. Some individuals simply seek to obtain direct financial gain through digital advertisements, as engagement with fake news messages about COVID-19 can be very high. The number of new domains and websites related to COVID-19 soared at the start of the pandemic[4].

Another strategy to profit financially from the COVID-19 crisis was to spread fake news about potential cures for the virus or effective prevention measures. Such messages also facilitated criminals seeking to sell items that they claim will help prevent or cure COVID-19, which emerged both on the Clearnet and the Darkweb.

The hybrid nature of this threat underlines the importance of a combined, hybrid response, especially considering that law enforcement agencies are not typically mandated with investigating cases involving disinformation or fake news, despite their potential to bolster criminal activities.

1.3 DATA COMPROMISE

The majority of threats discussed within the IOCTA ultimately pertain to some form of data compromise. As a result, data compromise is not dealt with as a separate category within the different chapters but rather emphasised within this cross-cutting chapter. Data compromise gathers significant attention through the obligation of organisations to report data breaches under the General Data Protection Regulation (GDPR). GDPR considers the protection of data belonging to EU citizens, thus it has an 'extra-territorial effect' applying to companies outside the EU who handle data relating to EU visitors[5]. Since the enactment of GDPR, over the past 18 months over 160 000 data breach notifications have been handed in to authorities[6], and a growth in interest over personal data handling among EU citizens[7]. In its annual data breach investigations report, Verizon reports how the company collected 157 525 incidents and 108 069 breaches[8]. The authors, however, immediately place these figures within their proper context as 100 000+ of those breaches concerned credentials of individual users. These are breaches where criminals target the users' credentials to gain access to bank accounts, cloud services, etc.

Data compromise therefore can refer to the ability of criminals to access individual user credentials or to access large databases with potentially valuable information. Examples of the latter include data breaches at companies that often become public knowledge. Both of these situations are not mutually exclusive, and often form a starting point for subsequent criminal activity. The majority of interviewees from law enforcement authorities and private sector representatives mentioned social engineering as a top threat, which cuts across different crime areas, affecting both cyber-dependent and cyber-enabled crime and illustrates the key role played by data compromise.

Social engineering

Social engineering and phishing remain a key threat. Based on interviewee responses, both demonstrate a significant increase in volume and sophistication. While some of the increase may be attributable to improved reporting mechanisms, it has also become

Law enforcement case study

European law enforcement conducted an investigation of ten cases of fraud related to technical support scams. The perpetrators initially communicated mainly via telephone with their victims, pretending to be technicians at a software company support centre. Under the pretext that their computer and/or mobile device are "infected" by malware, criminals asked the victims to install remote access software to allegedly solve the issue. In this way, the criminals gained full access to the computer or mobile device and consequently to the - stored on the devices - personal data. Through use of the personal data, the perpetrators transferred money from the electronic bank accounts (e-banking) to bank accounts controlled by themselves or their accomplices. In many cases, they even demanded the installation of remote management programmes on the victims' mobile phones, so that they could receive text messages (SMS) with the one-use codes (OTPs), which financial institutions send for security reasons. The investigation identified four individuals who were active or involved as money mules.

easier for technically inexperienced criminals to carry out phishing campaigns using existing criminal infrastructure and support services – a trend that is expected to continue in the future.

Targeting human weakness in the security chain, social engineering and phishing have a high impact on society and enable the majority of cybercrimes, ranging from scams and extortion to the acquisition of sensitive information and the execution of advanced malware attacks.

While criminals typically employ social engineering to convince targets to engage in fraudulent schemes unknowingly, criminals use phishing to either distribute malware or to obtain credentials and gain access to sensitive accounts and systems.

More sophisticated and more targeted phishing

A key trend over the past year relates to the growing sophistication[9] of phishing. Phishing has become more difficult to detect, with many phishing emails and sites being almost identical to the real ones. At the same time, phishing campaigns have become faster and more automated, forcing respondents to act quicker than before as in some cases it takes one day from a credential leak to an attack.

Overall, cybercriminals are employing a more holistic strategy to phishing by showing a high level of competency concerning the use of tools, systems and vulnerabilities they exploit, assuming false identities and working in close cooperation with other cybercriminals. Regarding the latter, criminals have shown their sense for innovation, as they use shared platforms to distribute their scams, which makes blocking or tracing difficult for incident responders. Criminals have also been observed maintaining a level of situational awareness, with a number of phishing campaigns having taken advantage of the COVID-19 pandemic[10].

Further to this, criminals have also employed a much more targeted approach when attacking their victims. Advanced actors focus more on selected victims as opposed to a random group in order to optimise financial gains, as they are becoming increasingly specialised in information gathering and victim profiling activities. As the main threat relates to spear phishing, criminals have proven apt at adapting their attacks to a specific context for fraud schemes in particular, for instance by improving their language skills or even using local 'customer agents' who communicate with their victims speaking their regional accents, or by making reference to current cultural, political, and local events.

In addition to employing a targeted approach, cybercriminals are adopting a more agile approach, constantly looking to harvest data and sensitive information from victims, which they can use to enable additional crimes. Lack of security awareness and a significant amount of open-source intelligence surrounding personal information of employees of businesses available online enable criminals to gather the information they need. Other forms of personal information harvested and abused by criminals may include financial and personal details, as well as login credentials for various sensitive accounts.

The majority of social engineering and phishing attacks are successful due to inadequate security measures potentially in combination with a lack of awareness by the users. Particularly the latter was highlighted repeatedly, as attacks do not have to be necessarily complicated or advanced to be successful – badly set up attacks still succeed by exploiting people as the weak part of the security chain. Accordingly, basic cyber hygiene and improved user awareness are some of the key success factors in curbing part of this threat.

Finally, cybercriminals are demonstrating an improved overall level of operational security and proving to be highly aware of how to hide their identities and criminal activities from law enforcement or private sector companies. In some cases, once a phishing attempt is being investigated, the whole criminal infrastructure has already vanished. Similarly, criminals may put in place technical measures to avoid suspicion. Through their deny/allow[11] lists of internet protocol (IP) addresses, for instance, criminals may forward the user to the genuine website if certain conditions are met (i.e. access through a computer, instead of a mobile phone, or from foreign IP address). As such, only the users selected as targets by criminals are re-routed to the phishing site.

CaaS as a facilitator of phishing and other forms of cybercrime

Cybercrime-as-a-Service (CaaS) facilitates phishing. Offerings on the Darkweb help criminals significantly improve overall technical complexity of their attacks without the need for advanced technical understanding. In recent years, CaaS has increasingly enabled even technically inexperienced criminals to carry out phishing campaigns by providing exploit kits, access to compromised systems and vulnerable remote desktop protocols (RDPs).

Here, criminals have also been reported to make increased use of legitimate commercial services such

Bust of hacker group selling databases with millions of user credentials

Polish and Swiss law enforcement authorities, supported by Europol and Eurojust, dismantled InfinityBlack, a hacking group involved in distributing stolen user credentials, creating and distributing malware and hacking tools, and fraud.

On 29 April 2020, the Polish National Police searched six locations in five Polish regions and arrested five individuals believed to be members of the hacking group InfinityBlack. Police seized electronic equipment, external hard drives and hardware cryptocurrency wallets, all worth around €100 000. The police closed down two platforms with databases containing over 170 million. The hacking group created online platforms to sell user login credentials known as 'combos'. The group was efficiently organised into three defined teams. Developers created tools to test the quality of the stolen databases, while testers analysed the suitability of authorisation data. Project managers then distributed subscriptions against cryptocurrency payments.

The hacking group's main source of revenue came from stealing loyalty scheme login credentials and selling them on to other, less technical criminal gangs. These gangs would then exchange the loyalty points for expensive electronic devices.

The hackers created a sophisticated script to gain access to a large number of Swiss customer accounts. Although the losses are estimated at €50 000, hackers had access to accounts with potential losses of more than €610 000. The fraudsters and hackers, among them minors and young adults, were unmasked when using the stolen data in shops in Switzerland.

as encrypted email and messaging applications as well as Virtual private network (VPN) providers to hide criminal activity, exploiting increasingly privacy-oriented policies, which make it difficult for law enforcement to gain relevant information in time.

Often, these less obvious legitimate services are safer for criminals to use and minimise risks associated with using underground services more commonly used by criminals in the past.

1.4 CRYPTOCURRENCIES FACILITATE PAYMENT FOR ALL FORMS OF CYBERCRIME

The abuse of cryptocurrencies continue to play an important role in facilitating payments for transactions across all areas of cybercrime. Reliability, irreversibility of transactions and a perceived degree of anonymity have made cryptocurrencies the default payment method for victim-to-criminal payments in ransomware and other extortion schemes, as well as criminal-to-criminal payments on the Darkweb. These activities have been long established with Silk Road emerging in 2011 and Cryptolocker hitting its first victims in 2013.

At that time, more than 20% of transactions were directly attributable to criminal activity. Although the level of criminal abuse has grown substantially, the legitimate use of cryptocurrencies grew at a much faster rate. In 2019, the overwhelming majority of bitcoin transactions were linked to investment and trading activity so, despite considerable abuse, criminal activity corresponds to only 1.1% of total transactions[12]. The figure includes transactions stemming from fraudulent activities, Darkweb trade, thefts and ransomware.

Criminals continue to use cryptocurrency as a method of payment for extortion activities

Although Initial Coin Offering scams and a wide range of Ponzi schemes abusing the increasing popularity of cryptocurrencies dominated criminal abuse by volume, most of the crimes reported to law enforcement included various forms of extortion. The last two years have seen an increase in extortion spam, where the suspect attempts to frighten the victim with a promise of a devastating event should they not receive payment in cryptocurrency, typically bitcoin corresponding to hundreds or even thousands of euros. While in its most basic form the suspect simply expects naïve victims to trust the threat, a slightly more advanced approach includes victims' passwords, typically leaked from one of the large public data breaches.

The extortion scam typically involves sextortion, theft of data or, more recently, COVID-19 related threats. While the majority of the population is immune to such attempts, criminals still seem to benefit from the activity. The scalability of cybercrime compared to traditional forms of crime presents a key challenge, as cybercriminals can target a relatively large number of potential victims with relatively low investment, being able to profit despite a small percentage of responses. According to a recent study analysing a subset of 4 million intercepted sextortion emails, over 12 500 bitcoin addresses were extracted, 245 of which received one or more payments[13]. Although such efficiency is much lower than observed across ransomware campaigns, it is still much more lucrative when compared to traditional low-tech scams.

Cryptocurrency users also target of criminals

The growing adoption of cryptocurrencies increases the number of vulnerable victims, so it is no surprise that thefts from individual and enterprise wallets have become more prominent over the last few years. In 2019, there were 10 publicly confirmed hacks of exchanges where criminals stole cryptocurrencies, resulting in a theft of €240 million worth of assets. Although the number of incidents was higher than in any of the previous years, the total amount stolen decreased compared to the previous year with €950 million stolen in 2018, including almost €500 million stolen from Japanese exchange Coincheck[14].

Cooperation with the private sector

While a massive effort has taken place in the cryptocurrency industry to deal with proceeds from criminal activities, the exchanges still differ in the degree to which they address the issue and the level of assistance they provide to investigators. In order to assess the players across the industry, Europol is

conducting the first international law enforcement survey[15] addressing the issue of cooperation with the major cryptocurrency exchanges and payment services.

The cryptocurrency industry and exchanges in particular have continued strengthening their know your customer (KYC) measures, either through their increasing effort to identify rogue clients or by a growing set of legislation affecting the industry.

In Europe, the most important legislative development in this area was a transposition of the 5th Anti-Money Laundering Directive. The Directive states that cryptocurrency exchanges and wallet providers who own private keys of their clients are obliged entities, mandating them, among other things, to a proper identification of their clients. The Directive obliges all European Union Member States to implement the legislation by January 2020. Twenty countries have implemented it on time[16] with more doing so throughout this year. While individual countries were given a large degree of flexibility when transposing the Directive, this development contributed to a much-needed harmonisation of legislation.

The number of cryptocurrency automated teller machines (ATMs) is continuously growing and surpassed 9 000 ATMs around the world in 2020[17]. Traditionally, ATMs have often been perceived as a way to privately obtain or sell cryptocurrency. Nevertheless, compliance also gradually improves, as an increasing number of operators require customer identification and flag suspicious transactions.

Challenges to feature more prominently in future investigations

A large number of factors have rendered cryptocurrency investigations more challenging and we can expect these to feature more prominently in future investigations. These include centralised and decentralised mixing services, privacy coins, exchanges with insufficient KYC requirements, clandestine over-the-counter trading, nested services, where the exchange is incorporated within a wallet or another service and decentralised exchanges.

The obfuscation methods continue to develop. Centralised mixers troubled with exit scams and high fees seem to be gradually replaced by non-custodial mixing solutions where users do not need to send bitcoins to a third party. Privacy-focused services

Looking ahead: Malicious use of artificial intelligence

Artificial intelligence (AI) is at the heart of the so-called 4th industrial revolution and promises greater efficiency, higher levels of automation and autonomy. AI is intrinsically a dual use technology: while it can bring enormous benefits to society, AI can also enable a range of digital, physical and political threats. Therefore, the risks and potential criminal abuse of AI systems need to be well understood in order to protect against malicious actors.

For instance, criminals could make use of AI to facilitate and improve their attacks by maximising opportunities for profit in a shorter time, exploiting new victims, and creating more innovative criminal business models, while reducing the chances of being caught. As 'AI-as-a-Service' becomes more widespread, it lowers the entry barrier to criminal activities by reducing the skills and technical expertise needed to employ it. This further exacerbates the potential for AI to be abused by criminals and become a driver of crime. Concrete scenarios include AI malware, AI-supported social engineering, AI-based password guessing, AI-aided reconnaissance or AI-facilitated content creation, to mention a few.

It is therefore necessary, in close cooperation with industry and academia, to develop a body of knowledge on the potential use of AI by criminals with a view to better anticipating possible malicious and criminal activities facilitated by AI, as well as to prevent, respond to, or mitigate the effects of such attacks in a pro-active manner. Understanding of capabilities, scenarios, and attack vectors is the key to enhancing preparedness and increasing resilience.

aside, the bitcoin protocol itself is expected to soon implement features that will make it less transparent to casual observers and investigators alike.

Cybercriminals will increasingly turn to marketplaces that support decentralised transactions. More marketplaces are likely to deprecate the traditional centralised model with deposit and escrow accounts in favour of direct transactions between buyers and sellers, decreasing the influence of market administrators and discouraging exit scams.

1.5 CHALLENGES WITH REPORTING PLAGUE ABILITY TO CREATE ACCURATE OVERVIEW OF CRIME

Several interviewees indicated how they are unable to provide a comprehensive overview of the number and types of crimes executed within a particular crime area. This is the result of a number of factors. First, the ability to register a specific crime is not always possible. Crime registration systems are diverse, and several interviewees indicated they were in a process of advancing their ability to gather more specific crime reporting data, i.e. specifying what type of cybercrime took place. In one Member State, ransomware, for example, was not a separate category, as the country maintains a general category for data breaches. Having a general code for data breaches led to classification problems, according to the Member State representative, as different types of crimes fall into the same category.

Second, victims often do not report the crime. Crime reporting is a general problem as such receives attention as part of a broader Victim Rights Strategy[18]. 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. Moreover, the more victims report a crime, the more data law enforcement can gather and the more likely connections between different crimes can be established. One of the interviewees indicated how under-reporting prevents law enforcement from forming the bigger picture and gathering reliable data, and monitoring whether cybercrime has been increasing or decreasing in reality.

Cryptocurrency as an investigation opportunity

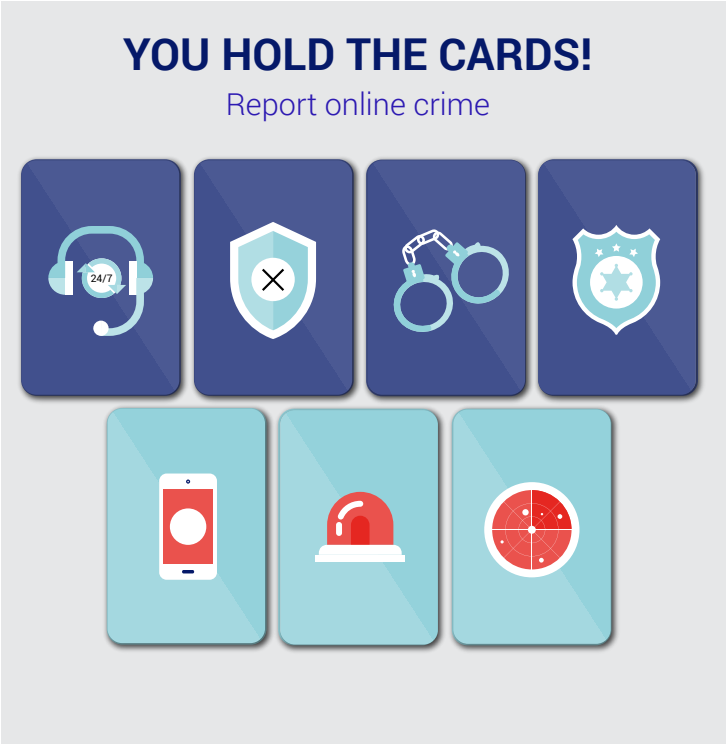
Cryptocurrency investigations have become an essential tool for many cybercrime investigators. While the role of Europol is to support investigations in the Member States, we could no longer ignore a high demand for relevant practical training. To cope with an increasing demand for a hands-on e-learning experience Europol in cooperation with CENTRIC launched CRYPTOPOL, an educational game for investigators in October 2019. CRYPTOPOL is accessible to all law enforcement cryptocurrency investigators around the world who can contact Europol to request access to the game. As the game contains information about tracing techniques used by law enforcement there is no intention of making it publicly available.

The other explanation for a lack of reporting from victims, at least with respect to the general public, is a lack of awareness. One interviewee indicated having witnessed a significant increase in cybercrime figures, but offered as an explanation that it may in fact be the result of greater awareness from the public. Others indicated there is no incentive to report as the focus is on business continuity.

Third, law enforcement at a national level often find out about a potential case through the media or through their local police. Crime registration at local police level maintains its own challenges as local police units may not have the expertise to assist a victim of cybercrime. Additionally, the information reported to local police may not find its way to national or central units, meaning law enforcement at is unable to connect the dots on a national scale and with their respective international partners.

Cybercrime in the media

Law enforcement officials also indicated using media as a source of crime reporting, which is not the preferred method as such reporting maintains its own challenges. Cybercrime is a complicated area filled with technical elements and cross-cutting issues,



which make it difficult to create a clear picture of the landscape. A lack of understanding of key terms, concepts and a limited viewpoint have shaped the way mainstream media have portrayed cybercrime to wider audiences. Sophisticated emerging technologies, human-relatable narratives, and high-profile cases (vis-à-vis victims or perpetrators) tend to dominate media headlines.

The complexity and terminological challenges of cybercrime can lead to inconsistencies between what the media reports and what the security community says about an incident. It is also not helpful that many companies name the same groups or attacks differently, enhancing the potential confusion. The complexity can lead to the perception of cybercrime as a highly sophisticated and intelligent field of crime. However, while for some cases this is an accurate assessment, this perception may lead to neglect of the human element of cybercrime, which is much less complex to comprehend. Additionally, there are many forms of cybercrime which are relatively unsophisticated, but which have substantial impact nonetheless. Cybercrime has a genuine human impact and individuals can do a lot to improve their resilience against different kinds of cyber threats if they are aware of them. Reporters may lack a coherent understanding of the cybercrime field, often mixing cyber-enabled fraud with cyber-dependent crime.

Where a high-profile incident occurs, an excessive focus on such cases may lead to indirect re-victimisation and, in some cases, directly casting blame on the victim, which harms investigations. Law enforcement view the media highlighting the more dramatic cases, while often ignoring the low-value but high volume cybercrime. When victims are essentially the only possible source of information in criminal cases, they are not likely to be willing to share information on their victimisation. This is particularly true with BEC and ransomware. Media reporting can turn the incident into a scandal story, which could lead to further victimisation and reputational damage.

Using media for awareness raising

According to law enforcement and private sector respondents, due to the receptive nature of several media outlets, there is substantial room to work collaboratively with media to raise awareness of neglected areas of cybercrime which have a substantial impact on EU citizens. There are extensive calls to have clearer, more accurate representation of cybercrime to public audiences. Law enforcement are calling for prevention to be covered more extensively. If done right, the media could become a powerful actor in cybercrime prevention, for example by exposing the adoption of new kinds of technologies and methods by cybercriminals.

Law enforcement has reported good reception among media representatives in raising awareness of concrete cybercrime issues. Active presence on social media by law enforcement, and sending out notices on cybercrime, is often well received by media and the public[19]. The media often picks up and shares the story.

This is important, as, for example, phishing and social engineering attacks rely on convincing humans to fall for fraudulent activities, which makes raising awareness on these threats potentially more impactful than focusing on disseminating high profile incidents. As national media outlets often spearhead media reporting in Member States, it would be important for the public and private sectors to engage with them regularly, raise awareness and communicate elaborately the realities of the threat landscape, which could help boost resilience against threats. People usually report crimes more after certain information is disseminated on threats.

1.6 LAW ENFORCEMENT ACCESS TO DATA CONTINUES TO CHALLENGE INVESTIGATIONS

For several years now, the advancement and increased implementation of certain technological developments have complicated the ability of law enforcement to gain access to and gather relevant data for criminal investigations. One of the most prominent examples in this regard remains the widespread use of encryption, which contains many benefits from a security perspective but is also a development that criminals have gratefully used to their advantage[20]. Europol has spoken about this in previous iterations of the IOCTA and jointly with Eurojust in its dedicated Observatory Function reports in 2019 and 2020.

Encryption continues to become a mainstream feature of an increasing number of services and tools. One example is the Domain Name System (DNS) over Hypertext Transfer Protocol Secure (HTTPs). DNS is one of the most important databases in the internet infrastructure. Increased concern over the monitoring of DNS traffic has led to the standardisation of modern DNS resolution protocols that make use of encryption. One of the protocols, which received increased popularity and adoption is DNS over HTTPS (DoH), after being introduced as a default setting on the application level. Even though the DoH protocol was created to solve historical DNS concerns regarding security and privacy, the potential centralisation of DNS traffic around a handful of commercial and private organisations has arisen as a result. Tracing historical DNS records is an effective tool when it comes to criminal investigations. Access to DNS queries is also used to great effect in dealing with botnets. Access to the network traffic between the criminal source and the remote DNS service provider, however, will now barely be possible due to traffic encryption, which will make the detection and blocking of malicious traffic, botnets and other malicious applications impossible.

As queries to the DNS will be encrypted, ability to gain access to such data will be more complicated for law enforcement, and countries hosting the majority of the DoH service providers will receive the vast majority of the internet DNS lookups, compared to the previous national decentralisation of these sensitive queries.

As a consequence of this, most of the DoH-related investigations will involve international legal requests to those jurisdictions. The DoH provider is likely to have a privacy policy in place, which will make it even more difficult for law enforcement to receive the necessary information for crime investigations. Finally, while positioned as a privacy-enhancing technology, it still allows internet service providers (ISPs) to profile users as other data points of the Hypertext Transfer Protocol (HTTP) traffic remain unencrypted.

Other related developments include the use of cryptocurrencies by criminals, as indicated earlier in this chapter. Whereas law enforcement, including Europol, continues to focus on improving capabilities in the area of cryptocurrency tracing, significant challenges remain.

Encrochat investigation provides new insights into organised crime

The value of being able to access data of criminal communication becomes most apparent when law enforcement succeeds in gaining such access. The case of Encrochat, an encrypted phone network widely used by criminals, is perhaps the most effective illustration of how encrypted data can provide law enforcement with crucial leads beyond the cybercrime area. It should be emphasised that the platform targeted by this investigation catered specifically to the needs of criminals. The phones using the platform were provided pre-configured and advertised to meet the needs of criminals and to secure the users against surveillance or investigation methods used by law enforcement parties. The phones are sold guaranteeing anonymity utilising a network of re-sellers, which are often themselves involved in other criminal activities, and are not distributed via regular retail outlets. In early 2020, EncroChat was one of the largest known providers of encrypted digital communication with a very high share of users engaged in criminal activity. User hotspots were particularly present in source and destination countries for cocaine and cannabis trade, as well as in money laundering centres. In July 2020, Europol reported on a joint investigation which made it possible for law enforcement to intercept, share and analyse millions of messages that criminals

While the activities on EncroChat have ceased, this complex operation shows the global scope of serious and organised crime and the connectivity of criminal networks who use advanced technologies to cooperate on a national and international level. The information has already been relevant in a large number of ongoing criminal investigations, resulting

in the disruption of criminal activities including violent attacks, corruption, attempted murders and large-scale drug transports. Certain messages indicated plans to commit imminent violent crimes and triggered immediate action.

This investigation confirms that advanced technologies enable criminals to secretly communicate or transfer illicit goods and resources. There is a growing risk to public safety as organised crime are drawn to using encrypted communication platforms that are almost technically impossible for law enforcement to access. Due to these emerging technologies used by criminals and the opportunities new technology may pose for law enforcement, an even more intense thinking beyond law enforcement cooperation is required, including with the private sector.

While the dismantling of EncroChat is a considerable success against serious and organised crime and the result of a multi-national investigation, the ingredients needed to come to such a success include the ideal combination of information, resources, skills, partners and opportunity. This means this type of success is an exception as the rule remains that law enforcement continues to battle the challenges of criminal use of advanced technologies.

Bulletproof hosters are the backbone of criminal infrastructure

An important building block of the criminal infrastructure is bulletproof hosting (BPH) – an essential CaaS offering, which continues to be a crucial facilitator for criminals and a hindrance for law enforcement by challenging identification and attribution efforts. BPH refers to a type of hosting or hosting provider that earns its money by consciously accepting perpetrators of crime as part of its clientele, offering them technical infrastructure resilient to law enforcement disruption or takedown. There are some hosting providers who may be negligent in acting on illegal content or criminal activity hosted by them, which is also an area of concern for law enforcement; however, the hosting providers that consciously act in or support the interest of the criminals ought to be the primary focus. These providers make their willingness to support criminal activity part of their appeal and their business model. This is a crucial advantage for criminals as hosting providers can play a central role in allowing criminal activity to continue.

As an infrastructure element, BPH facilitates a broad variety of key threats, including CSAM, terrorism-related content, command and control (C&C) servers used in cyber-attacks as well as platforms for criminal-to-criminal trade and discussion[21]. It is linked to several threats in cyber-dependent and cyber-enabled crime, making it a key concern in the threat landscape. As such, both the private and public sectors have a key role to play in hindering a BPH criminal application. This calls for cooperation internationally, as well as an appropriate legislative framework which would hinder BPH providers from acting maliciously by hosting criminal interests. For example, regional internet registries, local internet registries and ISPs have a significant responsibility in maintaining data accuracy when sub-allocating IP addresses to network operators in order to maintain traceability, with regard to combatting BPH, as IP addresses have a substantial role in BPH.

BPH providers may run their own static servers to host malicious content of their clients. BPH services have also registered as resellers with low-end service providers (for example ISPs, large hosting providers and content delivery networks) due to low-level verification and authentication requirements. With the growth of cloud services, a new modus operandi has emerged in which threat actors rent virtual private servers from legitimate hosting providers using fake or stolen identities. This highlights the need for stronger KYC policies with businesses and organisations across the sector.

Case example

In September 2019, German law enforcement managed to identify and arrest the main suspect running a BPH service from a bunker. This BPH facilitated illicit marketplaces for various kinds of drugs, CSAM and CaaS. Specifically, the WallStreet Market and Flugsvamp 2.0 were able to run on the servers of the bunker in Traben-Trarbach, Germany[22].

2

CRIME PRIORITY

Cyber-dependent crime

KEY FINDINGS

- Ransomware remains the most dominant threat as criminals increase the pressure by threatening publication of data if victims do not pay.
- Ransomware on third-party providers also creates potential significant damage for other organisations in the supply chain as well as critical infrastructure.
- Emotet is omnipresent through its versatile use as it leads the way as a benchmark of modern malware.
- The threat potential of DDoS attacks is higher than its current impact in the EU.

2.1 INTRODUCTION

The clear majority of law enforcement respondents named ransomware as a top priority threat yet again. As reported in previous years' IOCTA reports, ransomware remains one of the, if not the, most dominant threat, especially for public and private organisations within as well as outside Europe. Besides ransomware, European law enforcement reported malware in the broader sense to be widely present in cybercrime cases. Malware attacks on organisations that play a crucial role in the supply chains of major organisations have been a significant development over the past year. The third threat, the DDoS attack, celebrated its 20th anniversary in 2019 and ongoing investigations show that the DDoS threat is still prevalent in the cyber landscape.

2.2 RANSOMWARE

The clear majority of law enforcement respondents named ransomware as a top priority threat yet again. As reported in previous years' IOCTA reports, ransomware remains one of the, if not the, most dominant threat, especially for public and private organisations within as well as outside Europe. What makes it even more challenging as a threat, is the impact it has on its victims. This victimisation goes beyond the primary target, most often a public organisation or private business, as ransomware also affects those whose data is compromised. Considering the scale of damage that ransomware can inflict, victims also appear to be reluctant to come forward to law enforcement authorities or the public when they have been victimised, which makes it more difficult to identify and investigate such cases. With ransomware, criminals do not only abuse encryption to hide their identity and obfuscate their financial transactions but also actively abuse encryption as part of their modus operandi. This leads to a situation where they can almost act with impunity.

Ransomware is becoming increasingly targeted

Criminals continued the trend introduced last year by making their ransomware attacks increasingly sophisticated and more targeted. The number of targeted ransomware cases has increased over the past year, which has led to a significant increase in threat actor capability as well as a higher impact on victims.

Ransomware attackers continue to target public and private sector organisations of various size, industry and nationality rather than individual personal computers (PCs). This enables threat actors to increase both the ransom amount requested and the probability of successfully making the victim pay the ransom. Victim reconnaissance plays a significant role in the preparation of an attack. European law enforcement and Europol have observed attacks targeting local governments and ministries; other public sector organisations in healthcare and education (including hospitals, universities and high schools); as well as businesses in manufacturing, finance, energy, and transport industries. While the context of the COVID-19 pandemic crisis has affected the cybercrime field, ransomware attacks targeting the healthcare industry took place well before the crisis had a substantial effect in Europe and the US, which suggests that the COVID-19 crisis was not a trigger for these kinds of attacks[23]. What COVID-19 brought was an increase of the attack surface, with unmanaged endpoints/devices (PC systems) being remotely connected and having access to companies' information technology (IT) infrastructure. The 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. This gap has subsequently provided new ways for cyber-actors to gain access to companies' IT infrastructure.

Typically, ransomware attacks deployed against large corporations occur in different stages and are executed by different threat actors. The first initial step (performed by one group of criminals) of a ransomware infection is the computer/network intrusion which is done by the use of multiple attack vectors and malware types. The access is then sold to different cybercriminals that perform IT infrastructure mapping, privilege escalation, lateral move, data exfiltration etc. and finalised by deploying the ransomware.

Ransomware and third-party providers form a lethal combination

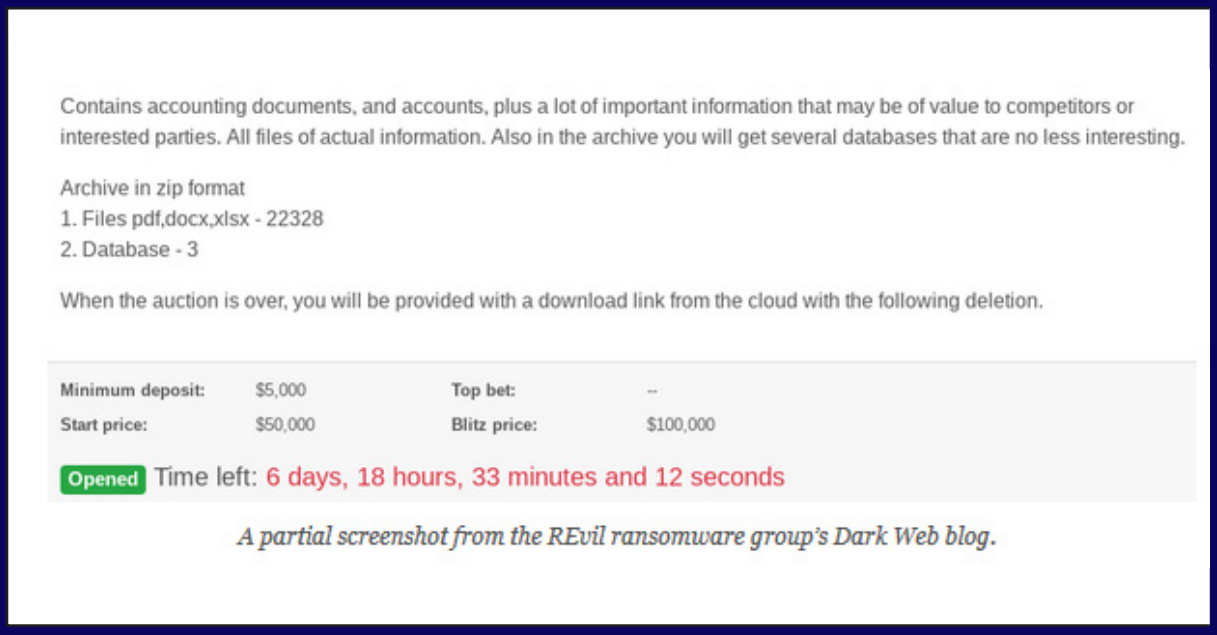
Ransomware has shown to pose a significant indirect threat to businesses and organisations by targeting supply chains and third-party service providers. Europol has followed up on attacks on organisations playing a key role in the supply chains of major financial institutions, which are believed to be an attempt by the attackers to enhance pressure on the victim to pay the ransom. Private sector respondents reported concerns over the differences in the IT security apparatus across supply chains, which leaves companies that play a key role as a service provider vulnerable to attacks. These attacks then have an impact across the whole supply chain, which may do substantial damage through long downtime or information leaks for organisations indirectly affected by the attack. One case saw an IT service provider being attacked with Maze ransomware, which can sit on the victim's servers for several months. This allows criminals to perform reconnaissance by monitoring internal communications in order to identify a key moment, such as merging, selling, big meetings with customers/sales, etc., for the deployment of the ransomware. Criminals deploy the ransomware before such events with the aim of putting pressure on the victim. At the same time, criminals can also exfiltrate

the data prior to the deployment of the ransomware to have another means of pressuring the victim. The existing presence of the criminals on the victim's servers is difficult to identify by security investigators as the security measures mainly focus on inbound detection.

A perverse twist to guarantee payment: threatening to auction or wipe data

Ransomware attackers have introduced a new way of pressuring their victims to pay by stealing the victim's sensitive data and threatening to publish it online. Once criminals gain a foothold on victims' networks, which can be done in various ways, they explore the networks and exfiltrate data, before delivering the ransomware. If the victim fails to pay the ransom demand, attackers will post the victim's sensitive data online or sell it to the highest bidder. The group behind Sodinokibi ransomware has already attempted to auction data which it gathered from a ransomware attack[24]. According to Member States and private sector respondents, several ransomware families including Sodinokibi (also known as REvil), Maze, Doppelpaymer, Nemty and Snatch published data which criminals stole from their victims over the past year. In particular, the auctioning of the data by criminal groups marks a new step and demonstrates an escalation in methods aimed at coercing victims to pay the ransom. It is anticipated that other groups will begin to adopt these coercive measures too.

Additionally, in the 2018 IOCTA Europol predicted scenarios in which fines for violating the GDPR could be used by threat actors as additional leverage with regard to the threat of leaking their victim's data online[25]. Both Member States and private sector respondents witnessed this phenomenon over the past year. Some ransom notes specifically mention GDPR fines to enhance the pressure on victims.



A partial screenshot from the REvil ransomware group's Dark Web blog.

Fig. 1 A screenshot of a data auctioning session online[26].

An alternative to the publication of data is its destruction. Some ransomware families, such as NotPetya have destructive wiper functionalities which may cause irreversible damage to the victim. Europol observed a case of destructive malware which took place in 2020, in which attackers managed to rewrite the master boot record.

Investment costs for criminals increase, but so do the potential profits

While the overall investment cost of ransomware is increasing, the amounts extorted by attackers have increased too. Attackers who launch ransomware attacks have requested ransom from anywhere between less than a thousand to millions of euros. The damages caused by e.g. downtime have increased significantly as well. When targeting their victims, European law enforcement found attackers surveying their victims and assessing both the victim's capacity

to pay (by reading e.g. financial reports) and the most effective way of infecting as many machines as possible during the attack. Attackers have also used encrypted communication means (such as Protonmail, Tutanota and cock.li) and set up customer service portals – many times a hidden service on Tor darknet – to help facilitate the extortion process.

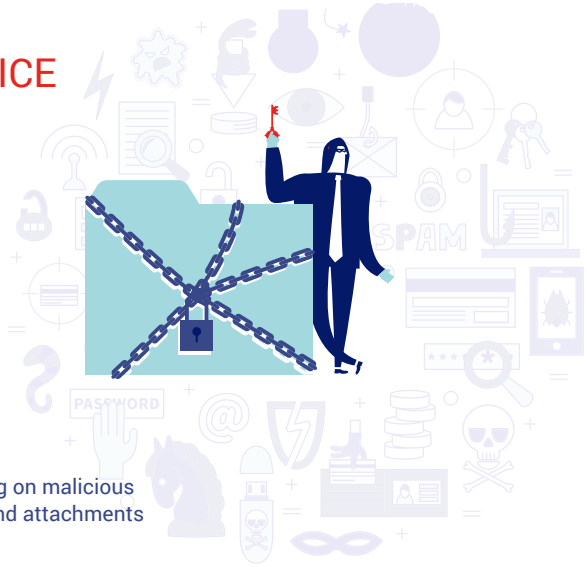
Ransomware attackers are becoming increasingly innovative in pursuing profits from the crime area. In addition to shifting to corporate and organisational targets and finding new ways of adding leverage to their extortion, threat actors are seen collaborating with other criminals and adding new layers to their attacks, including crypto mining. Increasingly professional affiliate schemes are reflected in the increase in migration among criminal affiliates, as was seen with the migration from GandCrab to Sodinokibi.

Ransomware attacks display higher skill, sophistication and adaptivity among threat actors

Ransomware attacks continue to be a relatively diverse, low risk and easy way for cybercriminals to acquire money. The level of sophistication also varies across threat actors. European law enforcement reported at least two distinct types of ransomware actors: lone actors who utilise data and services from Darkweb market places, who demand ransom up to five thousand euros; and well-organised crime groups with better technical capabilities targeting higher-value targets for ransom of up to millions of euros. Threat actors have displayed significant adaptability in conducting lateral movement, reconnaissance and in establishing new footholds. Several stages are still executed through more manual steps (and again by using legitimate tools) where lack of strong internal controls and logging does not expose and reveal the suspicious activities. The availability of Ransomware-as-a-Service (RaaS) on Darkweb marketplaces has also decreased the barrier of entry for new, less skilful criminal actors. Lockbit, for example, which emerged in January 2020, was brokered on underground forums for other cybercriminals to use[27]. However, on the opposite side, already established and mature RaaS actors have raised the bar by including only trusted affiliates into affiliate programmes. These trusted affiliates have previously displayed the capacity to infect large companies. Affiliates that cannot infect large companies or are inactive on the platform for more than one week are expelled (e.g. Sodinokibi).

The business-type nature of ransomware attackers is also demonstrated in their engagement in online public relations activities. Some ransomware groups conduct their own information campaigns to advance their goals. The Maze ransomware group for example released a statement on their website claiming that they would 'spare' healthcare organisations during the COVID-19 pandemic crisis. This turned out to be

Ransomware | TIPS & ADVICE



THE MALWARE THAT HOLDS YOUR DATA HOSTAGE FOR A PRICE

Ransomware prevents users from accessing their system or devices, asking them to pay a ransom through certain online payment methods by an established deadline in order to regain control of their data.

HOW DOES IT SPREAD?

- Visiting compromised websites
- Clicking on malicious links and attachments
- Downloading fake application updates or compromised software
- Connecting infected external devices (such as USBs) to your computer system

disinformation, as the group allegedly attacked an urgent care centre in Texas soon after their release (refusing to pay ransom, Maze continued to publicise stolen patient data)[28]. The Maze group was also allegedly behind an attack on the Hammersmith Medicines Research facility in the UK, who have been involved in developing vaccines for the COVID-19 virus[29].

Both Member States and private sector respondents have noticed an increase in subcontracting and cooperation among threat actors, which has improved their capabilities. 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. Well-organised criminal groups who engage in ransomware, have been observed by European law enforcement cooperating over malware, infrastructure and money laundering activities. The relationship between Emotet, Ryuk and Trickbot is considered one of the most notable in the cybercrime world.

Some ransomware actors have also grown more cautious. Member States and private sector respondents reported that some of the actors behind ransomware attacks have become less vocal on underground forums, setting up alerts and alarms. They have also been observed using additional VPN layers and cryptocurrencies with mixers and swappers to hide their tracks. According to European law enforcement, attackers have also found a way of using C&C servers when deploying malware to place the payload into the memory of the company's servers. This way there is no trace on the victim's hard disk and no way of recreating it once it is gone from memory. The IOCTA 2018 and 2019 include a section on file-less malware as an emerging threat in cyber-dependent crime, and the IOCTA 2018 included a forecast that file-less malware would become an increasingly standard component of CaaS offerings by 2023.

Ransomware remains an under-reported crime

Several law enforcement authorities mentioned identifying ransomware cases through (local) media and approaching victims to assist them by potentially starting a criminal investigation. This was not generally a priority of the victim organisation, as the primary focus was on business continuity and limiting reputational damage (see Chapter 1). The shift in ransomware targeting individual PCs to more high-value targets such as businesses and public sector organisations introduces unique challenges to law enforcement investigations. Private and public sector victims of ransomware are disproportionately more affected by the threat of leaking data compared to ransomware cases in which PCs and individual persons were affected. Negative publicity leading to reputational fallout may lead to re-victimisation, which may prevent victims from coming forward to law enforcement authorities with information which could be crucial in identifying and catching the perpetrators. Victims prefer to engage with private sector security firms for investigating the attack or negotiating with the extortionists to manage the crises triggered by ransomware (some IT security firms hire specialist negotiators, some of whom get discounts from organised crime groups). Some of the companies that negotiate the ransom payment are working on the edge of legality, as they have developed a trusted business relationship with the ransomware actors.

Companies are normally referenced by cybercriminals in their negotiations as a proof or ledger that the victim's data will be decrypted after the ransom payment. Some of these companies negotiate behind the scenes with the ransomware actors to obtain a bigger discount from the ransom payment. Other companies might reflect this discount in the victim's invoice, others may not. Cyber actors provide ransom discounts to victims if they use the services of specific companies. By using such companies, victims will not file an official complaint, which increases the lack of visibility and awareness concerning real figures of ransomware attacks among law enforcement. Not reporting cases to law enforcement agencies will obviously hamper any efforts, as important evidence and intelligence from different cases can be missed.

Furthermore, a case involving personal computers being targeted by ransomware shows that victims had opted to purchase new machines rather than report the event to law enforcement. Here victims were stunned when they were contacted by law enforcement over the ransomware attacks, and were under the impression that law enforcement would not do anything about the situation.

2.3 MALWARE

Besides ransomware, European law enforcement reported malware in the broader sense to be widely present in cybercrime cases. Criminals have converted some traditional banking Trojans into modular malware to cover a broader scope of collection of PC digital fingerprints collection and are being sold to cover different needs (e.g. droppers, exfiltration, etc.). These advanced forms of modular malware are a top threat in the EU. According to European law enforcement, incidents have been steadily increasing over the past year and are likely to rise significantly later in 2020. Malware typically includes Trojans and remote access tools (RATs), which allow criminals to gain remote control over infected computers. Some threat actors use techniques similar to those in the past in some cases resurrecting old exploit codes when taking advantage of hygiene security issues, such as the targeting of unpatched structured query language (SQL) vulnerabilities, making traditional attack methods still worthwhile.

The level of complexity varies across malware attacks. Several groups have proven more adaptive and capable than others. Some groups can utilise malware to attack higher value targets with a more targeted approach, performing research and reconnaissance on their victims, whereas other less experienced actors engage in lower impact, massive attacks.

Malware attacks have been targeting third-party providers

Malware attacks on organisations that play a crucial role in the supply chains of major organisations have been a significant development over the past year. Similarly, with ransomware, other forms of malware targeting third-party or outsourced service providers put supply chains at significant risk, as the impacts of such attacks could involve data leaks or major disruptions, as well as knock-on or cascading effects. Private sector respondents reported a growing number of attacks on third-party service providers; however, it is unclear whether attackers intended to impact the supply chain in all cases.

Ransomware case example

Criminals targeted a London-based foreign currency exchange Travelex with Sodinokibi ransomware in the first weeks of 2020. The company had over 1 000 stores and 1 000 ATMs in over 26 countries. Travelex was also a third-party service provider for several well-known financial institutions internationally. As the attack left Travelex's services disrupted for several weeks, this had varying impacts across the whole supply chain. The criminals encrypted Travelex's data and allegedly managed to exfiltrate five gigabytes of sensitive data from Travelex, including personal data, social security numbers, dates of birth and payment card information, which it subsequently threatened to make public if Travelex did not pay the ransom. The company managed to restore its operations soon after, but it was reported that Travelex paid the USD 2.3 million ransom to the attackers. It is not advisable for victims to pay the ransom, as there is no guarantee the victim will gain their data back nor that similar attacks will not happen in the future.

In one case, a private sector respondent reported one of their third-party service providers had been targeted by Emotet malware which led to a high-risk situation at the respondent's organisation. Attackers were studying old email threads between the targeted company and the respondent carefully, trying to embed themselves into the conversation naturally using highly tailored messages to gather information. Staff at the respondent's organisation grew suspicious when new names and email addresses were following up on months old threads, and so they reported the messages as suspicious. This case shows that threat actors put considerable effort and preparation into an attack.

Emotet leads the way as the benchmark of modern malware as malware variants evolve

The evolution of Emotet and Trickbot malware shows how adaptive the malware threat is. The Emotet banking Trojan – which is mentioned as the top malware threat affecting the EU by both Member States and private sector respondents – has been used by cybercriminals to deliver other malicious malware payloads such as Ryuk ransomware and Trickbot. The developers behind Trickbot added a 'Trickbooster botnet' (a spam booster) to the malware. These developments signal an evolution in the malware and their capabilities.

European law enforcement case study

European law enforcement have witnessed some perpetrators using trusted third-party services in their malware attacks, including Amazon Web Cloud and Google Drive. The most downloaded PowerShell scripts are online text paste tools, such as Pastebin. These scripts are then executed in memory, making forensic analysis more difficult (what is known as file-less malware). Using phishing emails or malware payloads, threat actors are using the legitimacy of these services to trick their users. While this modus operandi has been around for a few years already, 2019 saw a significant development. Cybercriminals hack legitimate sites (for example those run on WordPress) to house various payloads and malware, using them as 'stagers' to upload malware and phishing sites within them.

Emotet is highly professional and aggressive as it seeks to maximise its profits. Private sector respondents suggest Emotet is a benchmark for modern malware with over 200 000 unique versions observed globally. The group behind Emotet seems to take long breaks over the summer and when they return in the autumn, they become highly active again. Other top malware threats affecting Europe as reported by private sector respondents include Lokibot, which stores login credential information from web browsers and data related to cryptocurrency wallets, and Qakbot, another modular banking Trojan known to facilitate ransomware infections on corporate networks.

Crime-as-a-Service (CaaS) enhances reach of attacks

Prolific malware, which criminals turn into commodity malware for others to use, is cause for concern. Threat actors collude with one another by sharing infrastructure, services and compromised credentials. Commodity malware and Malware-as-a-Service (MaaS) lower barriers for threat actors wanting to engage in cyber-attacks.

Despite a substantial decrease in exploit kits on underground markets, prolific malware such as Emotet and Trickbot have successfully filled the void. Both Emotet and Trickbot use modular structures to enable reselling and renting sections of their malware to their rivals without compromising their key differentiators. "TrickBot likely is operated by a single group as a MaaS platform that caters to a relatively small number of top-tier cybercriminals. Available information leads us to believe that individual TrickBot campaigns can be attributed to these different customers using the group tag parameter, and each customer may bring their own tactics, techniques and procedures and engage in highly targeted attacks[30]."

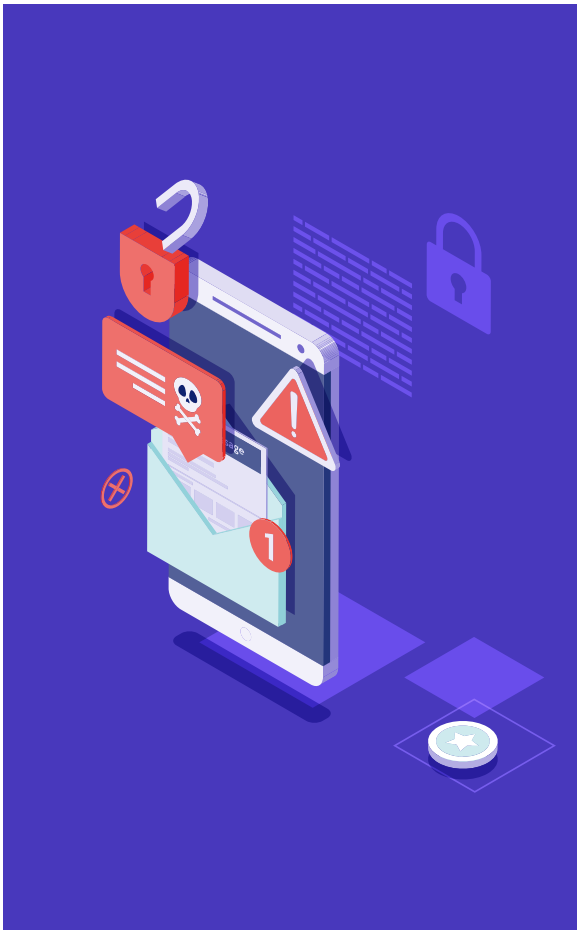
By doing the heavy lifting in acquiring access to a target's systems, Emotet can provide Access-as-a-Service (AaaS) to other cybercriminals. These other criminals can focus on monetising the opportunity with some other second stage malware. Competing solutions for electronic skimming (e-skimming) and JavaScript skimmers, with varying capabilities, each with the goal of compromising online merchant websites by harvesting payment card data, have also been offered as a service on the Darkweb by cybercriminals. These will be elaborated further in Chapter 4.

Simultaneously, European law enforcement has reported a rise in less tech-savvy cybercriminals in the context of widely available CaaS solutions. There has been an observable shift from what used to be a business for threat actors, now being more of an enterprise. Where specialist skills are needed (e.g. malware-coding, malware-distribution), criminals are able to hire developers or consultants to fill this need. This highlights increased professionalisation in the cybercrime threat landscape.

Through using combination attacks, criminals effectively challenge law enforcement's capacity to investigate incidents and attribute attacks to specific perpetrators and crime groups. Malware combinations add layers of complexity to law enforcement investigations. Encryption also presents a challenge, as malware developers often use encryption to frustrate law enforcement and industry efforts in analysing the functionality of malware and assign attribution to specific crime groups.

Mobile malware remain relatively stable

As more and more cashless payment transactions have emerged in the mobile scene, mobile threats such as mobile malware targeting cashless payment methods continue to grow. Mobile malware has yet to reach scalability as a sustainable business for cybercriminals, at least when contrasted with traditional banking Trojans. This is likely due to the limited transactions (with a cap typically set at around €50) which are enabled with mobile payments. Launching mobile malware attacks requires significant effort compared to other attack varieties which further offer larger payouts, which means they are likely conducted by less funded, amateur actors. European law enforcement also detected first signs of mobile payment fraud with attempted fraudulent transactions using app-based systems. Investigations are underway and it is unclear currently whether this involved mobile malware.



2.4 DDoS

In 2019, the DDoS attack celebrated its 20th anniversary. Ongoing investigations show that the DDoS threat is still prevalent in the cyber landscape. However, this topic has also had several success stories in prevention, mitigation and investigation. Attackers have adapted to these security measures by using attacks more efficiently, using both new tools and reigniting old techniques, and targeting more vulnerable victims.

Different types of attacks witnessed

Private sector and Member States respondents observed several phenomena relating to DDoS attacks over the past year. Private sector respondents reported seeing an increase in massive and simple DDoS attacks. European law enforcement did not witness significantly impactful attacks in 2019 but reported two kinds of attacks: targeted attacks which aim to damage specific industries or information systems; and crimes using automated tools. Automated attacks have been growing over the past year and are likely connected to CaaS. Threat actors can purchase pre-existing automated tools and deploy them for their own purpose, which makes conducting a DDoS attack a relatively cheap and easy way of carrying out an attack for threat actors who may have limited skills or experience in engaging in cybercrime. Moreover, criminals can use DDoS as a decoy or smokescreen for a more targeted attack.

Additionally, old DDoS methods are still prevalent. European law enforcement observed attacks targeting telecommunications and technology firms, where, in some cases, DDoS attackers threatened companies with reputational harm and extorted them for payment. Law enforcement agencies also came across cases where threat actors engaged in small attacks against larger organisations, extorting them for money with the threat of conducting larger attacks. Some threat actors targeted public systems and websites with DDoS attacks, however, these attacks were difficult to attribute to anyone specifically. One reason for the change in DDoS attacks could be the increase in protective measures used by organisations against them.

With respect to 2020, Amazon said its Amazon Web Services Shield service mitigated the largest DDoS attack ever recorded, stopping at 2.3 terabyte attack in February 2020[31].

DDoS has become increasingly adaptive

Cybercriminals 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. For example, private sector respondents reported smaller volume attacks which are capable of blocking smaller data centres. Small requests from 700 IP addresses make it difficult to block against a DDoS attack, and difficult for investigators to trace the attacker responsible as the attack comes from multiple IP addresses. These attacks incorporated additional methods which allowed the attackers to bypass the firewall's operational capacity.

Law enforcement case study

Law enforcement caught wind of a DDoS attack targeting a Finnish-based company. When approached by law enforcement, however, the company did not agree with the assessment, denying they were under attack. The attackers had used network mirroring DDoS via the Finnish company to amplify their attack on a major casino service in Southern Europe, which was the real target of the attack. Law enforcement thought that the Finnish company was the target, however attackers were only utilising the company's large network for mirroring and thus adding more volume to their actual DDoS attack. This is an old technique which has resurfaced after a few years, however with increased volume and capabilities. European law enforcement observed a couple of these cases.

IoT and DDoS

Connected devices, also known as the Internet of Things (IoT), are an additional avenue for DDoS attacks. According to private sector respondents, connected devices which run on legacy operating systems or which have weak or non-existent password protection could be vulnerable to DDoS attacks or for criminals wanting to provide DDoS services for other criminals, particularly as connected devices could be used for lateral movement to infiltrate networks. Private sector respondents also observed IoT botnets emerging, and while these have been mostly experimental, not yet witnessed in use for specific scenarios, criminals may advertise these for DDoS attacks.

The threat potential of DDoS attacks is higher than its current impact in the EU

Private sector respondents raised the concern of threat actors targeting third-party service providers with their attacks, for example energy and telecommunication providers. If attackers managed to bring down organisations in these sectors, criminals could potentially gain access to other valuable targets. Third-party service provider targeting could have other significant knock-on and cascading impacts in the supply chain. For example, the high level of interconnectivity in the financial industry also makes it vulnerable to disruptions.

3

CRIME PRIORITY

Child sexual exploitation online

KEY FINDINGS

- The amount of online CSAM detected continues to increase, further exacerbated by the COVID-19 crisis, which has serious consequences for the capacity of law enforcement authorities.
- The use of encrypted chat apps and industry proposals to expand that market, pose a substantial risk for abuse and make it more difficult for law enforcement to detect and investigate online CSE activities.
- Online offender communities exhibit considerable resilience and are continuously evolving.
- Livestreaming of child sexual abuse continues to increase and became even more prevalent during the COVID-19 crisis, a recent case shows CSAM production also takes place in the EU.
- The commercialisation of online CSE is becoming a more widespread issue.

3.1 INTRODUCTION

The main threats related to online CSE have remained relatively stable over recent years and throughout 2019. However, the COVID-19 pandemic has somewhat shifted this assessment. Detection of online CSAM was already increasing on a year-to-year basis, but saw a sharp spike during the peak of the crisis. A surge in the exchange of online CSAM occurred during the contact and travel restrictions and the consequences of this may have a long-term impact on CSE in general.

3.2 THE AMOUNT OF ONLINE CHILD SEXUAL ABUSE MATERIAL CONTINUES TO INCREASE

The year-on-year increase of detected online CSAM has continued. Law enforcement authorities in the EU see themselves confronted with an overwhelming amount of online CSAM to the extent that it becomes unmanageable for many of the units dealing with this crime. This includes regular complaints requiring investigation, including production of CSAM through rape and sexual assault, possession of that material, grooming, sexual coercion and extortion, but also referrals from the National Center for Missing and Exploited Children (NCMEC), ISPs, and hotline reports. This ongoing increase reflects a continuous distribution and redistribution of CSAM content. The effect of this on victims is significant and ongoing[32]. An international survey carried out by the Canadian Centre for Child Protection revealed that 70% of victims feared being recognised in public as a result of their involuntary participation in the offences against them[33].

The COVID-19 crisis revealed an extra surge in online distribution of CSAM. Referrals from the public, and industry in third-party countries reached record highs during the peak months of the pandemic. EU Member States also reported an increase in the number of blocked attempts to access websites featuring CSAM during their lockdowns. Moreover, several EU Member States have reported an increase in detected CSAM activity on Peer-to-Peer (P2P) networks especially in the second half of March, when lockdowns in EU Member States started materialising[34].

The increase in online CSAM has serious consequences for the capacity of law enforcement authorities to follow up and investigate reports of online CSE. Many investigators in EU Member States are faced on a daily basis with the task of making impossible choices between investigating one report instead of another.

There might be several reasons behind the growing amount of detected CSAM, including more offenders or better detection mechanisms. At least some of the CSAM is being repeatedly uploaded and widely distributed. However, the harm resulting from being a victim of this is severe, as victims experience repeat victimisation every time a picture or video is shared[35].

One of the drivers of the continuous growth of online CSAM is the growth in self-produced material. Especially during COVID-19 related lockdowns, children spent more time online, sharing images and videos that subsequently ended up with CSE offenders.

3.3 CRIMINALS INCREASINGLY ENCRYPT THEIR COMMUNICATIONS COMPLICATING INVESTIGATIONS

Offenders keep using a number of ways to disguise online CSAM, making it more complicated for law enforcement authorities to detect such images and videos. Although P2P network sharing remains among the most popular ways for perpetrators to share CSAM, it appears to be declining in popularity. The use of proactive EMPACT preventive and educative campaigns such as Police2Peer[36] seem to have had a continuing impact on reducing demand through these networks over time. One-to-one distribution and sharing among larger groups routinely takes place on social networking platforms and widely used encrypted communication applications such as WhatsApp, a trend reflected by the increasing number of referrals from US service providers via NCMEC[37].

Increased encryption of many digital communication channels means it is becoming more and more challenging for law enforcement agencies to investigate these crimes. There is increased activity on encrypted communication platforms beyond Tor, making it difficult to detect and investigate online CSE activities, including the creation and distribution of material, online grooming, sexual coercion and extortion.

Perpetrators have been using encrypted communications for a long time, but now even less tech-savvy offenders can easily use encryption. While the development of encrypted messaging platforms is not something bad in itself, it does raise significant obstacles for investigations in this crime type. Additionally, the conversion of popular unencrypted chat applications to encrypted status poses a substantial risk of increased abuse of those platforms for the exchange of CSAM and communication between offenders[38]. Several platforms including Facebook have reported a significant amount of CSAM. If these platforms move to implement end-to-end encryption for their messenger, concerns will rise over their continued ability to identify CSAM on their own platforms.

International police cooperation leads to the arrest of a Darkweb child sex abuser in Spain

The operation to bring down a child sex abuser, who had made explicit videos of an underage boy, owes its success to international cooperation. Information from Queensland Police – Australia's Taskforce Argos sent via Europol's secure communication channel – allowed Europol experts to carry out operational analysis, which revealed that a video from 2015 found in Belgium and France may have been filmed in Spain.

The analysis of the images and video – which showed how the suspect abused a boy who was under five years old at the time – led the Spanish National Police to locate the suspect. When looking into the message published with the video, officers noticed that the suspect used words and phrases from Spain and not from a Latin American country.

Using operational analysis, open-source enquiries and cross-checking information, Europol experts found that the suspect was registered on several websites and boards dedicated to child sexual abuse and exploitation on the Darkweb. The investigation revealed that the suspect was also using a social media network where he was in touch with a woman who shared the same surname as the one in the title of the sexual abuse video.

Once the abuser was located in Barcelona, cybercrime experts from the Spanish National Police Central High-Tech Crime Unit located in Madrid moved to Barcelona. Due to the lockdown in Spain, they were assisted remotely by other experts in Madrid. The material seized showed how the arrested suspect was using several email addresses and Darkweb access points to commit this crime[39].

3.4 DARKWEB OFFENDER COMMUNITIES ARE CONTINUOUSLY EVOLVING

Online offender communities exhibit considerable resilience in response to operational activities carried out by law enforcement agencies, attacks by unidentified actors and losses of staff and platforms. Their reactions include resurrecting old communities, establishing new communities, and making strong efforts to organise and administer them.

Parallel to the activity of large offender communities through Darknet forums is a development involving smaller communities sharing CSAM directly with each other via encrypted messaging platforms. Following several high-profile law enforcement operations on the Darkweb, many offenders seem to believe they are more secure in such small networks, sometimes based on invite-only. Offenders are also known to have used encrypted communication channels to infiltrate existing child-aged groups and form break-off groups involving children and adults[40].

In response to law enforcement operations targeting these Darkweb communities and due to the need to select participants and ensure exchanges of information are strictly related to child sexual abuse, offenders tightly control their communities. They use Darkweb forums as meeting places where participation is structured similarly to criminal organisations, with affiliation rules, codes of conduct, division of tasks and strict hierarchies. The purpose of the structure is to enforce rules and promote individuals based on their contribution to the community, which they do by recording and posting their abuse of children, encouraging others to abuse and providing like-minded, technical and practical support to one another.

Administrators require strict observance of the rules to avoid being banned from the forum. In addition, compliance with the rules and active participation can lead to a progressive increase in rank. Users regularly publish information and safety manuals aimed at avoiding detection by law enforcement authorities. Some users are also attentive to law enforcement operations and regularly publish news articles or even summary reports of the techniques used during successful operations. Cross-posting of such advice across various boards and forums highlights a collective approach to improve operational security for all. Some of these communities also meet offline, sometimes travelling great distances and bringing physical hard drives as storage media with them. Whereas Darkweb communities and real-life child sexual abusers used to be relatively separate, there appear to be more hands-on abusers – including individuals travelling for live distant child abuse – who are also very active on the Darkweb. Some law enforcement agencies have had cases where offenders keep material they produced themselves with them for many years before uploading it to the internet, hoping to avoid victim identification. This illustrates the crucial importance of victim identification efforts by law enforcement agencies, such as the Victim Identification Taskforce (VIDTF) organised on a regular basis by Europol.

Ninety suspects identified in major online child sexual abuse operation

Police around the world have taken down a global child abuse ring with links to over forty countries through a Belgian investigation supported by Europol. Four suspects have been convicted by a Belgian court.

This case was sparked by the Belgian East Flanders Federal Judicial Police, after more than nine million pictures and videos of the abuse of thousands of children from around the world were found there during a house search.

The vast majority of this footage had never been seen in circulation before by law enforcement. Suspecting they were producing their own, the Belgian investigators launched operation Gargamel together with Europol across Europe and beyond. The image and video data seized during this investigation has been used for Victim Identification Task Forces hosted by Europol, through which seventy children and thirty suspects have been identified. The Belgian Federal Judicial Police succeeded in identifying 60 suspects (of which 24 in Belgium) and 40 victims, which brings the actual total to ninety suspects and 110 victims.

Some suspects have already appeared before court in a number of other countries. In Australia, a suspect was sentenced to 15 years in prison.

More arrests and rescues are expected globally as police in over 40 countries examine the intelligence packages compiled by Europol and information from the Belgian Federal Judicial Police[43].

3.5 LIVESTREAMING IS BECOMING MAINSTREAM

Livestreaming of child sexual abuse continues to increase, becoming even more popular than usual during the COVID-19 crisis, when travel restrictions prevented offenders from physically abusing children[41]. As offenders had fewer opportunities to engage in physical CSE, live streaming emerged as a viable alternative to hands-on child sexual abuse. In some cases, video chat applications with built-in payment systems are used. This is a complicated area for law enforcement investigations, as usually none of the material is recorded, except for occasional chat conversations.

The Philippines remains the main country where live distant child abuse (LDCA) takes place. Cases of online CSE in the Philippines surged during the COVID-19 crisis, as the lockdown meant already poor families struggled to generate income and children did not go to school[42]. However, this year has further confirmed that this type of online CSE is not limited to Southeast Asian countries. A large operation in Romania uncovered significant levels of livestreaming taking place within the country, demonstrating that the EU is not immune to this threat.

In some cases, those seeking live streams of CSE are deceived: they pay for a live stream, but never receive anything.

3.6 COMMERCIALISATION OF ONLINE CSE IS AN EMERGING THREAT

Last year's IOCTA reported that commercialisation of CSAM remained limited to LDCA[44]. However, the past year has brought to light a number of indications that the commercialisation of online CSE is becoming a more widespread issue. For a long time, online CSE was one of the few crime areas Europol focused on that was not primarily driven by financial gain. Although offenders are still primarily driven by a desire to obtain more CSAM, in some cases they do seek to profit from online CSE. The emergence of a profit-driven model in this crime area is a worrisome development.

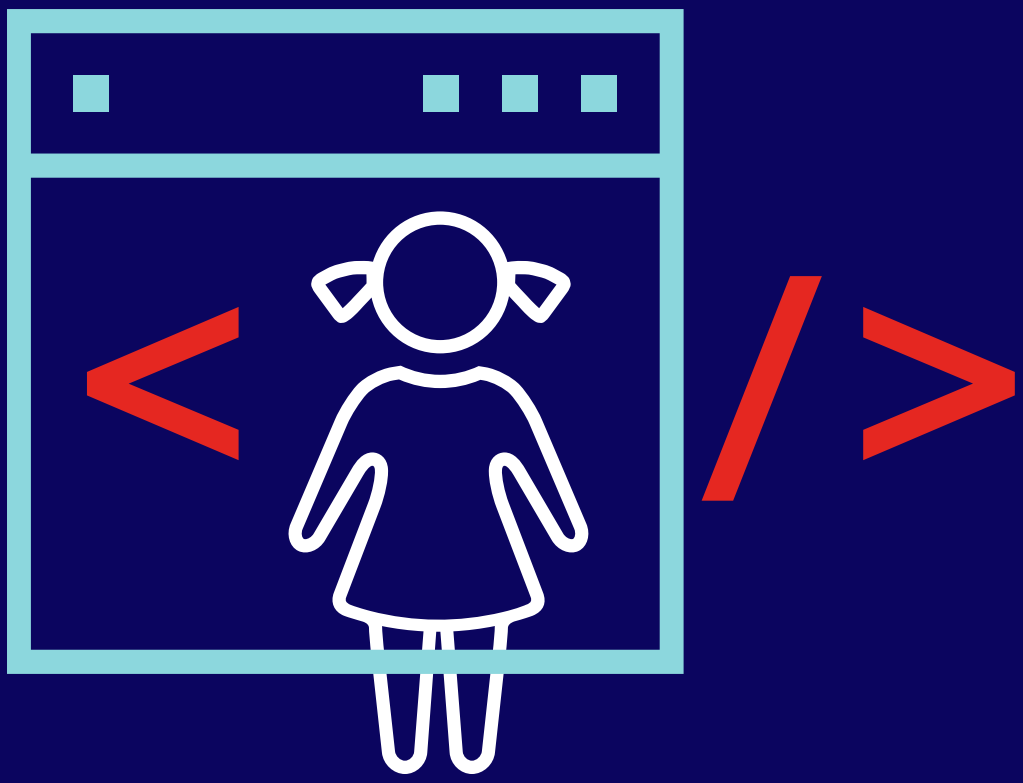
The monetisation of content has been seen on both the Clearnet and the Darknet, with many links on the dark web referring to Clearnet resources. Individuals monetise CSAM by uploading material to hosting sites (including legitimate hosting services) and subsequently acquiring credit on the basis of the number of downloads. This credit can be used to pay for additional hosting or in some instances can be cashed out, either in cryptocurrencies or other means. LDCA has had a commercial element for a longer time, as offenders frequently pay to watch parents, carers and offenders abuse children remotely to order. Uploading CSAM to legitimate hosting services is another method of monetising CSAM. The platform used to download this material may not be aware of the content or can claim not to be aware. The hosting site's advertising and the potential profits per click are also increased through such models.

3.7 ONLINE CHILD SEXUAL ABUSE TO REMAIN SIGNIFICANT THREAT

Online child sexual abuse remains a significant threat. The situation with COVID-19 has increased the time people spend online, whether it is for remote working, remote schooling or spare time. Children who spend a lot of time online unsupervised are therefore much more exposed to potential offenders through online gaming, the use of chat groups in apps, phishing attempts via email, unsolicited contact on social media as well as through less secure online educational applications[45]. Additionally, unsupervised time online further increases the risk of producing and distributing self-generated indecent material among underage individuals, which could also eventually reach child sex offenders. Furthermore, child sex offenders could take advantage of lonely and isolated children online, connecting with them to produce explicit material or to arrange a meeting in real life[46]. The current situation regarding COVID-19 creates considerable levels of uncertainty and unpredictability for the foreseeable future. The developments around the pandemic and related lockdowns and travel restrictions will have a big influence on the developments regarding online CSE.

The growth in CSAM being detected is showing no signs of stabilising, let alone decreasing. The end of the current health crisis and the lifting of lockdown measures may result in an increased number of reports of CSE, as abuse that occurred during the COVID-19 pandemic may be reported to law enforcement or other authorities after the fact. It is highly likely that in the upcoming year there will be a sharp increase in the amount of self-produced indecent material, which might also lead to a corresponding increase in online solicitation and exploitation.

Travel restrictions and other measures during the pandemic have likely prevented offenders from travelling and so have shifted their focus further to the exchange of CSAM online. A relaxation of travel restrictions and opening up of air travel will likely lead to an increase in transnational offenders seeking out CSE in certain countries and regions. If air travel remains limited for the foreseeable future however, or becomes more expensive, it is also possible we will see an increase in proxy offending both with surrogates such as childlike sex dolls or via live streaming.



4

CRIME PRIORITY

Payment fraud

KEY FINDINGS

- SIM swapping is a key trend that allows perpetrators to take over accounts and has demonstrated a steep rise over the last year.
- BEC remains area of concern as it has increased, grown in sophistication, and become more targeted.
- Many law enforcement agencies and financial services identified online investment fraud as one of the fastest-growing crimes, generating millions of losses and affecting thousands of victims from all EU countries.
- CNP fraud continues to increase as criminals diversify in terms of target sectors and e-skimming modi operandi.

4.1 INTRODUCTION

While the majority of fraud types are well known, they enjoy continued success due to insufficient cybersecurity measures and an overall lack of awareness. Fuelled by a wealth of readily available data, as well as a CaaS community, it has become easier for criminals to carry out attacks. As a result, law enforcement and industry continue to identify well-established frauds such as BEC, as a major threat but also witnessed new key trends such as SIM swapping emerge.

4.2 INCREASE IN SIM SWAPPING AND SMISHING

SIM swapping is one of the new key trends in this year's IOCTA. This modus operandi garnered considerable attention over the past twelve months, as law enforcement agencies noticed a significant increase with a growing number of cases in Europe.

SIM swapping is a type of account takeover and refers to the circumvention of SMS-based 2FA to access sensitive user accounts. Criminals fraudulently swap or port the victim's SIM to one in the criminal's possession in order to intercept the one time password (OTP) step of the authentication process. Since this typically requires detailed information on the victim, SIM swapping attacks are highly targeted. This also means that the overall volume of cases differs from Member State to Member State, leading to SIM swapping cases causing significantly higher losses in some jurisdictions while it is barely present in others.

Overall, SIM swapping poses a significant concern and huge potential danger and risk. A successful SIM swapping attack can lead to criminals gaining complete control over a victim's bank, email or social media account, and as a result, enable a number of serious follow-up crimes.

Operation Quinientos Dusim[47]

In January 2020, investigators from the Spanish National Police together with the Civil Guard and Europol targeted suspects across Spain believed to be part of a hacking ring which stole over €3 million in a series of SIM swapping attacks. Law enforcement arrested 12 individuals in Benidorm (5), Granada (6) and Valladolid (1).

Composed of nationals between the ages of 22 and 52 years old from Italy, Romania, Colombia and Spain, this criminal gang struck over 100 times, stealing between €6 000 and €137 000 from bank accounts of unsuspecting victims per attack.

The modus operandi was simple, yet effective. The criminals managed to obtain the online banking credentials from the victims of the different banks by through the use of banking Trojans or other types of malware. Once they had these credentials, the suspects would apply for a duplicate of the SIM cards of the victims, providing fake documents to the mobile service providers. With these duplicates in their possession, they would receive the 2FA codes directly to their phones send by the banks to confirm the transfers.

The criminals then proceeded to make fraudulent transfers from the victims' accounts to money mule accounts used to hide their traces. All this was done in a very short period – between one or two hours – which is the time it would take for the victim to realise that his/her phone number was no longer working.

Operation Smart Cash[48]

An eight-month-long investigation between the Romanian National Police and the Austrian Criminal Intelligence Service with the support of Europol has led to the arrest of 14 members of a crime gang who emptied bank accounts in Austria by gaining control over their victims' phone numbers.

Law enforcement arrested the suspects earlier in February in Romania in simultaneous warrants at their homes in Bucharest (1), Constanta (5), Mures (6), Braila (1) and Sibiu (1).

The gang perpetrated the thefts, which netted dozens of victims in Austria, in the spring of 2019 in a series of SIM swapping attacks.

Once having gained control over a victim's phone number, this particular gang would then use stolen banking credentials to log onto a mobile banking application to introduce a withdrawal which they then validated with an OTP sent by the bank via SMS allowing them to withdraw money at cardless ATMs.

It is estimated that this gang managed to steal over half a million euros this way from unsuspecting bank account owners.

Similar to SIM swapping, SMishing has seen an increase over the past twelve months. SMishing refers to the sending of fraudulent text messages purporting to be from trusted senders, typically targeting financial institutions and their customers.

SMishing is a lucrative alternative to phishing by email for a number of reasons. As most bank customers receive the advice to be suspicious of emails, customers do not yet have the same level of scepticism towards potentially fraudulent text messages. In addition, it is difficult to impossible for banks to protect their customers from SMishing attacks, as criminals aim to abuse the Alpha Tag of the SMS thread and Signaling System 7 (SS7) vulnerabilities.

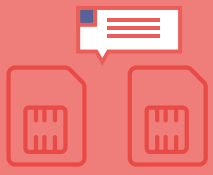
SIM SWAPPING – A MOBILE PHONE SCAM

SIM swapping occurs when a fraudster, using social engineering techniques, takes control over your mobile phone SIM card using your stolen personal data.

HOW DOES IT WORK?

A fraudster obtains the victim's personal data through e.g. data breaches, phishing, social media searches, malicious apps, online shopping, malware, etc.

With this information, the fraudster dupes the mobile phone operator into porting the victim's mobile number to a SIM in his possession



The fraudster can now receive incoming calls and text messages, including access to the victim's online banking

The victim will notice the mobile phone lost service, and eventually will discover they cannot log in to their bank account

WHAT CAN YOU DO?

- Keep your software updated, including your browser, antivirus and operating system.
- Restrict information and show caution with regard to social media.
- Never open suspicious links or attachments received by email or text message.
- Do not reply to suspicious emails or engage over the phone with callers that request your personal information.
- Update your passwords regularly.
- Buy from trusted sources. Check the ratings of individual sellers.
- Download apps only from official providers and always read the apps permissions.
- When possible, do not associate your phone number with sensitive online accounts.
- Set up your own PIN to restrict access to the SIM card. Do not share this PIN with anyone.
- Frequently check your financial statements.

ARE YOU A VICTIM?

- If your mobile phone loses reception for no reason, report it immediately to your service provider.
- If your service provider confirms that your SIM has been swapped, report it to the police.

Exploitation of 2FA behind smart ID

Three EU Member States reported cases of SMishing. Criminals used SMishing to bypass the 2FA mechanism offered by national smart IDs. Criminals aiming to attack bank accounts and the respective national banking infrastructure targeted these national Smart ID solutions through social engineering. Abusing alphanumeric SMS threads, criminals sent SMS appearing to come from the bank. These text messages prompted the recipients to log in to their online bank accounts using their smart ID, for instance to change their bank information. Following the link, they were then directed to fake bank log in account pages, which would verify a fraudulent transaction initiated by the criminal after they attempted to log in. Alternatively, threat actors would use this modus operandi to create a new Smart ID account under the victim's name, but under full criminal control.

4.3 BUSINESS EMAIL COMPROMISE REMAINS A THREAT AND GROWING AREA OF CONCERN

BEC remains a main and further growing threat for law enforcement and private industry. BEC is a sophisticated scam targeting businesses and organisations, whereby criminals employ social engineering techniques to gain access to an employee's or executive's email account to initiate bank transfers under fraudulent conditions, i.e. by pretending to be the CEO and asking the employee to carry out a payment.

BEC causes enormous losses and disruption to livelihoods and business operations[49]. Often following spear phishing emails, BEC is highly tailored and very effective with targets ranging from governments, international organisations, small to large businesses and individuals.

The two most common types of BEC are CEO fraud (criminals impersonating a high-level executive requesting urgent bank transfers) and invoice fraud (criminals impersonating suppliers asking for legitimate payments to be directed to a bank account under the criminal's control, or creating new, fraudulent invoices).

According to interviews with Member States, in many cases, BEC is carried out through a compromise of email accounts hosted by Office 365, access to which is typically gained through credential phishing in advance to the fraud. This is often possible due to limited security measures, such as a lack of 2FA; as well as a lack of awareness regarding spear phishing attempts. These type of attacks are still mostly originating from Eastern Europe, Nigeria and other African countries. The most sophisticated threat actors come from Israel.

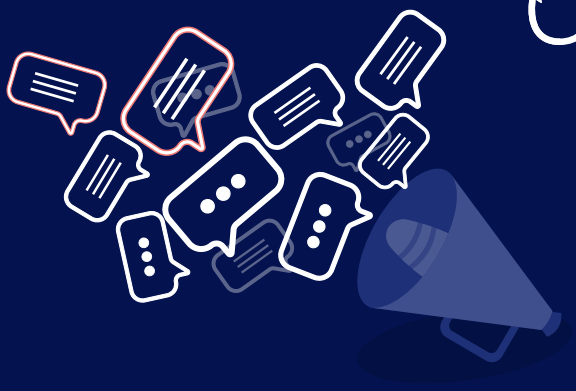
BEC has increased, grown in sophistication, and become more targeted

Over the past twelve months, BEC has increased across most EU Member States, with an additional increase as a result of the global outbreak of COVID-19. This increase in volume coincides with a growing sophistication and a more targeted approach. Criminals make use of technically advanced measures, such as compromising bank accounts, identifying the ideal time to strike, managing email conversations with complex man-in-the-middle attacks or even using Artificial Intelligence (AI) to mimic the voice of a company's CEO[50]. The growing sophistication of BEC is also reflected in the establishment and use of complex criminal networks, which are used to launder the proceeds of the fraud. Additionally, criminals have become better at local languages and the exploitation of local contexts.

While criminals target all kinds of organisations and businesses, there is an increased focus on smaller companies, rather than just large corporations. As a result, even cybersecurity companies not usually dealing with BEC have been receiving requests for technical assistance, for instance to conduct forensic investigations on the servers.

BANK SMISHING SMS

Smishing (a combination of the words SMS and Phishing) is the attempt by fraudsters to acquire personal, financial or security information by text message.



HOW DOES IT WORK?

The text message will typically ask you to click on a link or call a phone number in order to 'verify', 'update' or 'reactivate' your account. But...the link leads to a bogus website and the phone number leads to a fraudster pretending to be the legitimate company.

WHAT CAN YOU DO?

- Don't click on links, attachments or images that you receive in unsolicited text messages without first verifying the sender.
- Don't be rushed. Take your time and make the appropriate checks before responding.
- Never respond to a text message that requests your PIN or your online banking password or any other security credentials.
- If you think you might have responded to a smishing text and provided your bank details, contact your bank immediately.

Industry case study

A private sector partner reported a case in which a threat actor used social engineering and blended attacks to target the bank and its corporate clients simultaneously. The fraudster, having gained access to the client's email network, contacted the bank to request a change of the client's beneficiary account. The perpetrator subsequently managed the conversation and information exchange between the bank and the corporate client at the same time. Through this, the perpetrator showed a thorough understanding of the bank's processes and knowledge of who to speak to in order to change the account.

Industry case study

One private sector partner reported a case in which a criminal impersonated its CEO while at a conference. The threat actor made initial contact through WhatsApp, using a spoofed ID account and picture of the CEO and subsequently sent a forged email from the CEO about an urgent acquisition. Using information taken from open sources, the attack was highly targeted and convincing, demonstrating detailed knowledge about the CEO's current whereabouts. The fraud – the payment of an invoice, which never existed – was stopped only at the last moment, when a missing purchase order number raised a red flag.

Criminals likely to abuse voice biometrics

In the future, law enforcement and industry expect to see an increased use of voice biometrics to commit impersonation fraud. While biometrics are currently working well, attempts to compromise them to get access to bank accounts for BEC are expected to proliferate as additional security measures are being implemented.

4.4 ONLINE INVESTMENT FRAUD DRAWS IN VICTIMS ALL OVER EUROPE

Another relative 'newcomer' in this year's IOCTA is online investment fraud. Many law enforcement agencies and financial services identified online investment fraud as one of the fastest-growing crimes of the past twelve months, generating millions of losses and affecting thousands of victims from all EU countries. Many Member States witnessed this type of fraud for the first time.

Online investment fraud refers to a fraud type whereby criminals aim to lure their victims into transferring them money with appealing get-rich-quick schemes. Offering commodities such as cryptocurrencies, diamonds, or gold, criminals promise victims extraordinary financial returns on their investments, while criminals keep victims engaged through websites showing fake investment returns. While online investment fraud usually accounts for mid-level money losses, some victims have lost their entire life savings before realising that they had fallen victim to a scam.

Online investment fraud demonstrate high level of complexity

A number of online investment fraud cases have shown a significant level of complexity, with large networks of shell companies and call centres behind these schemes, as well as the development of software and communication tactics to systematise the exploitation of victims to their last cent.

In some cases, criminals have asked victims to install RATs to take control over the target computer, to initiate money transfers to criminals through full control over the computer and bank account. In addition to eliciting money transfers from their victims, criminals have also been seen to combine this type of fraud with phishing and the theft of credentials to be used subsequently for additional fraud.

Criminals usually target victims through social media, using celebrities and fake versions of news outlets, or come across the fraudulent investment web sites via search engines. Criminals have also been seen employing blended social engineering, with a mix of SMishing, cold calling and other techniques. Often these targets include older victims, who are less technologically savvy.

Online investment fraud is difficult to investigate, as criminals set up complex international schemes of companies with legal appearance, spanning across several legal jurisdictions. The groups behind these schemes are difficult to identify, due in part to their use of anonymisation tools, spoofed phone numbers and legitimate-looking websites.

Given the fast rise of investment fraud in many EU Member States, law enforcement agencies expect this type of fraud is to continue to increase and appear in so far unaffected countries, too. Perpetrators generally seem to originate from Russia, Ukraine and other Eastern European countries

4.5 CARD-NOT-PRESENT FRAUD CONTINUES TO INCREASE AS CRIMINALS DIVERSIFY

CNP fraud, such as carding and e-skimming, has increased over the past twelve months, with criminals shifting to new sectors and employing novel modi operandi.

Carding refers to the use of stolen card data to purchase goods or services. While carding has increased, criminals have moved away from targeting the airline industry towards the accommodation and rental sectors. The reduction in airline fraud is a direct result of successful public-private cooperation, which reduced the overall losses by nearly 50% and pushed criminals to other sectors. This is in addition to the purchase of goods such as mobile devices, phones and electronics, which criminals bring in from other countries using compromised card details.

Criminals take the stolen card details from dark web marketplaces (such as the Joker's Stash[51]), which make it increasingly easy to obtain stolen credentials from specific forums. Since these Darkweb forums typically require payment or some kind of interaction in order to gain entry, access is often difficult for law enforcement to obtain.

E-commerce/digital skimming a low risk and high-value modus operandi

The compromise of card data through e-skimming (also referred to as digital skimming) has increased, with technically knowledgeable organised criminal groups targeting e-commerce merchants with weak security measures. While sometimes criminals are seen targeting bigger companies when they see the opportunity, e-skimming mostly affects smaller to medium-size merchants, who do not have the capabilities to put into place sufficient protection and who, as a result, are often compromised without being aware of the criminal activity taking place on their sites.

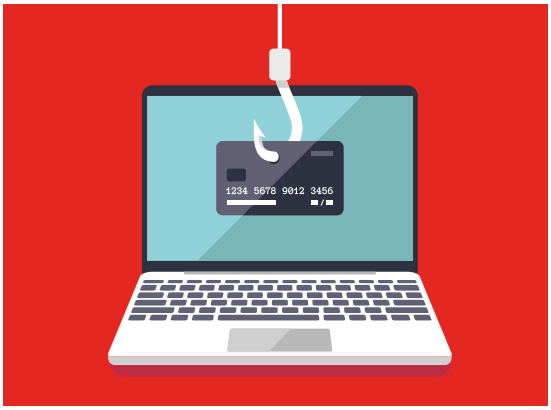
In an e-skimming attack, criminals inject malicious JavaScript code into the merchants' checkout pages, which allows them to capture personal data

Investigating carding on the dark web

During the Carding Action Week at the end of 2018, the Hungarian police launched an investigation into a vendor who was active on various markets offering card details from Hungarian cardholders.

The vendor was using different Pretty Good Privacy (PGP) public keys on the various market places but the police were able to decode these keys. This made it possible to identify the vendor's primary e-mail address used for registration on these market places.

During the investigation, the police were able to link the vendor's activities offering 400 account details from various financial institutions including 198 Visa accounts. Visa provided the necessary evidence and law enforcement arrested the vendor, and he is currently in custody waiting for his trial. The cooperation between the Hungarian Police and Visa resulted in the saving of €227 286 of potential fraud losses.



and credit card credentials. The malicious code typically checks the various customer and payment account number inputs, exfiltrates the data to an attacker-controlled C&C server, following which criminals can use this information to commit other crimes. Criminals commonly exploit for example improperly configured cloud data repositories, occasionally utilising automated processes to target vulnerabilities. Other entry points that criminals have increasingly been targeting include e-commerce merchants directly, or their service providers, which are supplying solutions ranging from analytics and advertisements to other general IT services.

The most common type of e-skimming activity, which interviewees mentioned, relates to the use of Magecart malware by organised criminal groups. This type of digital skimming has proven to be so lucrative that many established cybercriminals have moved into conducting such attacks, with JavaScript-based skimming now considered one of the main threats to financial institutions.

Private sector respondents have seen different variants of point of sale (POS) malware, including PwnPOS, AlinaPOS, and POSeidon / Backoff. FIN7 and FIN8 have been active threat actors in this area. FIN8 has also been observed using new malware toolsets to target POS environments.

As with other cybercrime areas, e-skimming, too, has seen criminals coming up with novel technical ways to execute their attacks, such as the Pipka malware.

Spotlight: FIN6

FIN6 is a prolific group of criminals, which has been targeting merchant point of sale (POS) systems to gather payment account data. In 2019, they expanded their attacks to e-commerce merchants, which represents a merger between CNP fraud and e-commerce breaches. The attackers injected malicious code into the merchant's websites, which would gather payment account number inputs and gather these account numbers into an attacker-controlled C2 server. Other skimmers have been observed gathering more input data than payment account numbers, which puts users' data at risk.

Spotlight: Pipka

Pipka is a new form of JavaScript skimmer which allows cybercriminals to configure which form fields the programme will parse and extract, including payment account numbers, expiration data, card verification values and the payment cardholder's name and address. Pipka has the added feature of being able to remove its malicious JavaScript component from the Hypertext Markup Language (HTML) code after successful execution. This is a new development in JavaScript skimming, and it adds interesting new layers to the malware. The Pipka skimmer reflects advancements made in e-skimming, and it goes to show that criminals targeting e-commerce will continue to develop innovative approaches to gather sensitive payment account data.

Darkweb marketplaces enable increase of e-skimming

Dedicated forums give cybercriminals the possibility to offload their stolen credit card data in a relatively low risk and efficient way. The forums also provide user-friendly interfaces for fraudsters seeking to buy them. At the same time, CaaS has created a competition between various underground forums, where cybercriminals are offering their sniffers and skimmers with constantly improved capabilities.

E-skimming poses a significant challenge to law enforcement and industry

While it is an increasing threat causing significant losses, detection of e-skimming is often difficult. Merchants do not necessarily realise that they have been infected, as it is the card-issuing banks that notice the frauds first. Reporting back to the merchant does not always take place, especially if the bank and the merchant are in different countries, in which case it can be difficult to determine who is liable for covering the losses: the bank or the merchant. In addition to the difficulty of timely detection, there are currently no anticipated technological or legal drivers to deter criminal groups conducting Magecart-style attacks, which is likely going to lead to a further increase in these types of attacks.

Digital fingerprints for sale

Continuing innovative developments of recent years, criminals are offering full digital user profiles in order to bypass advanced fraud prevention tools. In keeping up with e-commerce merchants increasingly employing analytics checking a user's identity against device fingerprints and several other metrics, criminals have moved to obtaining and selling these digital profiles to commit fraud. Taken from machines compromised in a botnet, they are used in order to make purchases using the compromised computer pretending to be a returning customer, using the same browser settings and victim's card credentials. After the fraud, many victims erase the evidence themselves, following Windows security guidance to restore to the last known configuration after having been compromised by the botnet, effectively removing all traces of the intrusion. This use of botnets to bypass sophisticated fraud prevention tools reflects a recurrent theme in the fight against cybercrime – as security measures are heightened, criminals come up with novel ways to continue their illicit activities.

4.6 TERMINAL ATTACKS INCREASE AS POPULARITY OF BLACK-BOX ATTACKS SOARS

Logical attacks on ATMs and POS devices remain a threat and have increased across most Member States. Among these, especially black-box attacks have proven popular, as organised criminal groups successfully manage to extract large amounts of cash in short periods of time. Black-boxing involves the installation of an external device connected to the cash dispenser in order to bypass the need for a card authorisation to dispense cash. Typically, the actual installation of the black box requires little technical knowledge besides the provision of the device and instructions. With cybercriminals remotely sending instructions to jackpot the ATMs, itinerant criminal networks are able to operate across several locations in different countries within a few days, requiring quick law enforcement response and international cooperation in order to stop them. These criminal groups are often Russian-speaking and with links to Eastern Europe, actively targeting ATMs across Europe.

Criminals are targeting mostly older ATM models, for which security measures and software have not been updated. While the modi operandi here remain largely the same; with occasional developments taking place in accordance with improved ATM security measures, law enforcement agencies noticed some changes in modi operandi over the past twelve months. As such, one Member State respondent saw a particularly ingenious criminal group using a new type of modus operandi for each attack, including a malware to check the balance of an ATM before deciding to attack it.

CRIME PRIORITY

5 The criminal abuse of the darkweb

KEY FINDINGS

- The Darkweb environment has remained volatile, lifecycles of Darkweb market places have shortened, and no clear dominant market has risen over the past year compared to previous years to fill the vacuum left by the 2019 takedowns.
- The nature of the Darkweb community at the administrator level shows how adaptive it is under challenging times, including more effective cooperation in the search for better security solutions and safe Darkweb interaction.
- There has been an increase in the use of privacy-enhanced cryptocurrencies and an emergence of privacy-enhanced coinjoin concepts, such as Wasabi and Samurai.
- Surface web e-commerce sites and encrypted communication platforms offer an additional dimension to Darkweb trading to enhance the overall business model.

5.1 INTRODUCTION

In 2019 and early 2020 a high level of volatility on the Darkweb was witnessed. Following protective measures, which multiple marketplaces have implemented, the situation has calmed down considerably. Nevertheless, the Darkweb environment remains difficult to disrupt as developments are often challenging to anticipate. This adds to the law enforcement challenges with respect to this growing threat, which continues to function as a key facilitator for many other forms of crime.

5.2 MARKETPLACE DEVELOPMENTS

More marketplaces based on purchased scripts have launched over the past twelve months, but some of these disappeared due to hacking or exit scams. The decrease in large-scale marketplaces has led to an increase in smaller marketplaces, in some cases catering to specific users or needs. Some of these markets are growing and as they gain positive feedback from users, they are becoming increasingly stable. Users are monitoring ratings and usually tend to keep to stable markets and vendors with high ratings. The market community has engaged in new ways of building trust with its users by developing cross-cutting solutions on information and reliability. A new site called DarkNet Trust has emerged which verifies vendors' reputations by searching through usernames and PGP fingerprints and it is able to search over ten thousand profiles from marketplaces[52].

After the takedown of DeepDotWeb mentioned in the IOCTA 2019[53], centralisation of information on Darkweb markets has stabilised and even increased. DeepDotWeb was a popular information service which made it easier for users to navigate the Darkweb ecosystem. Users are now looking to set up information hubs to increase user-friendliness in the Darkweb environment and sites such as dark.fail and darknetlive.com have taken over DeepDotWeb's role as information hubs. Dread, a popular Darkweb forum found on The Onion Router (Tor), continues to operate, having been around for approximately three years. The administrators of Dread additionally produced a DDoS protection solution (nicknamed Endgame Filter), which is free to use for other marketplaces, therefore expanding their role beyond a traditional information hub. Developers have also produced a Darkweb search engine termed Recon, a service allowing users to see what kind of drugs are for sale on the Darkweb, what vendors there are and what ratings they have. Another example of a Darkweb search engine is Kilos, which emerged in November 2019 reportedly as a potential follow up of Grams. Grams was a Darkweb search engine which ceased operations in 2017[54]. Since going online Kilos seems to have adopted the objective of indexing more platforms and adding more search functionalities than Grams. Moreover, Digital Shadows describes how "Kilos has introduced updates, new features, and services that aim to ensure security and anonymity for its users and also add a more human element to the site not previously seen on other prominent Darkweb-based search engines."[55]

Even though marketplaces continue to appear and disappear, an increasing number of operationally secure marketplaces, such as wallet-less and user-less markets, have emerged. Additionally, some marketplaces have intentionally relatively short lifecycles, which pose a challenge to law enforcement investigations. Short life cycles are making it difficult for law enforcement to investigate criminal cases. Administrators seem to want to stay under the radar of law enforcement by knocking down markets and keeping market lifecycles low.

Darkweb child abuse: administrator of Darkscandals arrested in the Netherlands

Early in March 2020, Europol announced the successful takedown of DarkScandals, a website which hosted videos of non-consensual and violent sex videos, including elements of rape, torture, human trafficking and CSE. The website had claimed it hosted thousands of videos of this kind of footage from all around the world. The Dutch law enforcement authorities and national prosecutor's office cooperated with German authorities, US law enforcement authorities and US Department of Justice and Europol in an operation to arrest the administrator and takedown the DarkScandals website. The administrator, a Dutch national, had allegedly received over 2 million dollars in exchange for selling the content on the website. The offender was charged with several counts of distribution of CSAM, production and transportation of obscene matters for sale or distribution, engaging in the business or selling or transferring obscene matter, and laundering of money instruments[59].

5.3 ADMINISTRATORS AND USERS ADAPT AS THEY AIM TO ENHANCE SECURITY AND RESILIENCE

Furthermore, Darkweb administrators have been observed pulling together and showing a collaborative spirit to maintain the environment under challenging circumstances. When faced with similar challenges, forum and service administrators have been seen working more closely together over sharing code and security methodologies (i.e. anti-DDoS measures, avoiding scams, creating trust-building sites to help users navigate vendors across different marketplaces, etc.). The Darkweb is essentially shaping into a 'business sector' in itself. There are also differences in the way administrators conduct their business on the Darkweb. Some are presenting to have a moral compass, banning items relating to the COVID-19 pandemic crisis, for example. This is not typical across the Darkweb, but it is an indication that some administrators differ in their approaches to conducting illicit trade.

Administrators are also looking to upgrade their security apparatus with other new features. Some marketplaces are already shifting to wallet-less and user-less markets, adopting multi signatures on Bitcoin and Monero, lacking registration requirements and enacting no JavaScript policies. Monopoly is also a wallet-less market in which payment occurs directly between buyer and vendor, and instead of enacting transaction fees, the market receives a monthly commission. Marketplaces were observed using multi signature wallets in their transactions[56].

Users have also opted to use safer communications methods. The reputation of Protonmail, an encrypted email service considered to be a former favourite among Darkweb users[57], has suffered after accusations that it has been helping law enforcement. Due to this, Darkweb users are shifting to new emerging encrypted email services such as Sonar and Elude[58].

In addition to encrypted email services, Darkweb users are relying increasingly on popular digital communication channels such as Discord, Wickr and Telegram. As these offer some degree of anonymity to the users, criminals consider it a safe place. This has introduced new initiatives, such as the Telegram vending service bot.

5.4 INFRASTRUCTURE PREFERENCES REMAIN STABLE, BUT CRIMINALS DO USE ALTERNATIVES

In terms of the Darkweb infrastructure, Tor remains the preferred option. As a result, criminal usage of Tor continues to be the primary focus. However, criminals have started to use other privacy-focused, decentralised marketplace platforms, such as OpenBazaar and Particl.io to sell their illegal goods. The emergence of decentralised privacy-oriented platforms is not a new phenomenon in the Darkweb ecosystem but they have started to increase interest over the last year. OpenBazaar in particular is noteworthy as certain high priority threats have emerged on the platform over the past year. These include those banned by some of the other Tor market-based administrators such as weapons and fentanyl. Even though the numbers may be considered limited, the nature of these items means the focus ought to be on impact rather than volume. COVID-19 related items also emerged on OpenBazaar during the pandemic. OpenBazaar has advertised a mobile platform Haven and has seen thousands of downloads on Android[60].

5.5 PRIVACY ENHANCING WALLETS EMERGE AS A TOP THREAT, AS PRIVACY ENHANCING COINS GAIN POPULARITY

With respect to cryptocurrency on the Darkweb, privacy-enhanced wallet services using coinjoin concepts (for example Wasabi and Samurai wallets) have emerged as a top threat in addition to well established centralised mixers. Apart from expected functionality including advanced decentralised coin mixing or integration of Tor these offer additional features. Samurai, for example, offers remote wipe SMS commands when under distress. These wallets do not necessarily remove the link between the origin and destination of the funds but certainly make cryptocurrency tracing much more challenging. Some administrators of underground markets are trying to apply these wallets to their payment systems. Threat actors have also been witnessed increasingly using hardware wallets, a separate physical device, which securely store seeds and private keys for a wide range of cryptocurrencies.

Initially, Darkweb markets relied solely on Bitcoin. However, over the past few years this has changed. An increasing number of markets are recognising the benefits of offering multiple coin alternatives, including Litecoin, Ethereum, Monero, Zcash, and Dash. While Bitcoin still remains the most popular payment method (mainly due to its wide adoption, reputation and ease of use), the use of privacy-enhanced cryptocurrencies has somewhat increased albeit not at the rate expected by their proponents. Monero is gradually becoming the most established privacy coin for Darkweb transactions, followed by Zcash and Dash. All these privacy coins may present a considerable obstacle to law enforcement investigations, despite the competing altcoin communities uncritically favouring their implementation over the others.

5.6 SURFACE WEB PLATFORMS OFFER AN ADDITIONAL DIMENSION TO DARKWEB TRADING

Some platforms existing on the clear web (or surface web) are also catering Darkweb goods and services, which offers additional benefits for criminals' business models. A number of cybercriminals are relying on surface-level e-commerce platforms for increased visibility, posting links to their online digital goods stores. One case involved an e-commerce platform registered to a company based in the Middle East, hosting online stores selling malicious digital tools from Arabic, Russian, and English language-based underground forums (links were found to underground forum administrators including cracked.to and nulled.to). Stores on the platform also offered stolen accounts, databases, carding, crypters, banking malware, ransomware and variants of the Mirai botnet. This platform allowed sellers to accept payments through PayPal and cryptocurrencies[61]. Surface e-commerce sites are useful for cybercriminals, as they allow them to showcase their products and services and they are legitimately registered businesses. Law enforcement also found cybercrime tools available on other clear web sites.

5.7 STEADY SUPPLY OF DIVERSE DARKWEB MARKET ITEMS

There has been an increase in the provision of digital and cybercrime elements on the Darkweb. Personal data, access to compromised systems (e.g. through RDP application), as well as services catering malware, ransomware and DDoS attacks, are all elements prevalent for the facilitation of cybercrime. Document and proof of identity services have also increased on the Darkweb. Perpetrators generally use identity and document services to support citizenship claims and other applications, obtaining lines of credit to set up a business, open untraceable bank accounts, proof of residence, to commit insurance fraud, purchase illicit items and other uses. There has been a shift in the offering of legitimate-looking counterfeit passports to "legal or registered" passports, which can pass several authentication tests, with criminals offering registered passport services. Trend Micro Inc. explains that the increase of global immigrants and the increasing adoption of e-passports is a likely driver behind this trend[62]. Additionally, some Darkweb sites also promote money laundering and instructions for users on how to use cryptocurrencies for money laundering.

Users can find drug listings in massive volume on the Darkweb; however, these do not necessarily reach priority-levels in terms of impact. More impactful, dangerous drugs, such as fentanyl, opioids and heroin are still significantly present on the Darkweb, although listings are smaller in number. Europol has observed an increasing trend of top organised crime groups having a presence on the Darkweb dealing drugs, which is likely due to an effort to expand their distribution mechanisms. As noted in IOCTA 2019, drug dealers may also be running multiple monikers on the Darkweb, which makes it difficult to prioritise within the drug topic. Additionally, the COVID-19 pandemic crisis seemed to have the most effect on the supply chains regarding drug trade compared to other crime. This has now stabilised and the situation has returned to normal, with an anticipated growth on the horizon.

Finally, the distribution of firearms has become significantly more fragmented. After the takedown of the Berlusconi marketplace by Italian law enforcement, which used to be the go-to place for firearms on the Darkweb, firearms have emerged on different marketplaces. Firearms are also available on OpenBazaar, although the scale of supply is unconfirmed. Some shops are also selling firearms from the United States. The ability for individuals to purchase firearms on the Darkweb has become increasingly difficult, due to recent law enforcement successes in catching individuals purchasing firearms illegally.

The diverse products and services vary in their level of impact and their ability to facilitate more serious forms of crime. The supply of these goods on the Darkweb poses a significant threat in the EU. Furthermore, the geographic nature of the threat is also diversifying. The Hydra market – the largest darknet marketplace serving Russia and neighbouring countries – has recently advertised an impending publication of a new, secure encrypted market platform, which they aim to open to the English-speaking community. Such a development would arguably make Darkweb investigations more difficult for law enforcement in the future and poses a significant threat to the EU.

Recommendations

The following section consists of highlights from this year's Member State and partner interviews combined with Europol insights. The majority of the responses resonated with previously reported recommendations focusing on recurring themes, such as:

» coordination and cooperation;

» information sharing
(removing practical obstacles, enhance judicial cooperation, reduce time, foster a culture of transparency and trust);

» enhancing the legal framework;

» prevention and awareness;

» capacity building.

Coordination and cooperation remain critical

There is little doubt that cybercrime requires more effective cooperation between private and public sector parties. Attackers use a coordinated approach and share infrastructure, which makes a broad and cohesive response to the criminal developments even more important. This also requires the engagement of multiple levels of collaboration.

More taskforce-like approaches, which has worked especially well in the Netherlands and the UK, would be beneficial. Considering the global nature of the Darkweb ecosystem and cross-border interaction of its users, the key recommendation is to establish a dedicated multinational Darkweb task force to approach the problem. This would help address legal jurisdiction challenges and obstacles hindering coordination.

Pre-investigative actions and information sourcing should be enabled with a dedicated centralised approach in the EU. This would help identify firstly priority cases and criminals, and secondly, appropriate jurisdiction over cases and highlight the most efficient ways of cooperating over specific cases and operations.

There is a persistent need for better cooperation with hosting services, social media platforms, and ISPs. Companies need to be more proactive in illegal content and activity and blocking it as soon as they detect it. One way of improving this is to invest in technologies that make sure their platforms are clean. They should also be able to demonstrate more willingness to assist law enforcement agencies to deal with, for example, CSE, and show improved openness and transparency.

Information sharing becomes even more crucial to offer timely response to cybercrime

Efficient and timely information gathering, analysing and sharing is crucial for fighting cybercrime. To this end, information sharing should be harmonised (what information can be shared between parties) and institutionalised. Structured efforts need to be put into place, increasing trust among the parties sharing information.

We must develop a culture of acceptance and transparency, and incentives for victims to bring their incidents to light and not fear penalties and re-victimisation for being targeted by cyber-attacks.

Considering the fast nature of cybercrime, it is important to make the exchange of information in light of international cooperation faster by implementing channels with, for example, the relevant ISPs at the European level (VPN, anonymisers, anonymous email providers, cryptocurrency exchanges, etc.).

Enhancing the legal framework

International law and national legislation should be better aligned with investigation practices in cybercrime. The link between legislation and investigative practices requires more focus.

There should be more relevant and focused legislation addressing bulletproof hosts and registrars, with which voluntary cooperation varies with law enforcement.

Darkweb threat actors increasing reliance on encrypted email services, privacy-enhanced cryptocurrencies and BPH providers pose a substantial problem to law enforcement. This calls for increased KYC type policies.

Prevention and awareness as well as crisis management

As indicated in many parts of the IOCTA, criminals remain successful because of inadequate cyber hygiene and an inability of victims to detect cybercriminal activities. This inability often stems from a lack of awareness on the side of the victim. This returns in many different forms of crime, including social engineering and phishing, as well as investment fraud. A lack of knowledge and awareness of the risk related to online CSE is also one of the drivers behind the increase in online CSAM. This highlights the need to continue promoting preventive and educational initiatives in a coordinated and structural manner across Europe.

In addition to raising awareness, there are calls for more effort on improving general cyber preparedness, including crisis management, exercises and disaster recovery plans. This is a recommendation which Europol in cooperation with its partners has responded to through its efforts with respect to the Law Enforcement Emergency Response Protocol (LE ERP). Developing evaluation schemes to assess and test IT security with infrastructure and devices, establishing rules and setting guidelines could increase resilience against cybercrime.

Capacity building

Cyber elements are becoming more and more visible in other areas of criminality and increasing numbers of these criminal activities are becoming cyber-enabled. This trend requires increased capacity among law enforcement to deal with this evolving challenge. Integrating cyber elements into law enforcement readiness already at the police academy level would enable educating and facilitating individuals who want to specialise in cybercrime. Effective investigations require technical expertise (civilian) and experience in criminal cases (law enforcement). Every police force should be responsible for developing knowledge within their units.

References

1 Durbin, Steve, "The Future's Biggest Cybercrime Threat May Already Be Here", https://www.darkreading.com/vulnerabilities---threats/the-futures-biggest-cybercrime-threat-may-already-be-here/a/d-id/1338439, 2020

2 Europol, "Staying Safe During COVID-19: What you need to know", https://www.europol.europa.eu/activities-services/staying-safe-during-covid-19-what-you-need-to-know, 2020

3 The European Union External Action Service (EEAS), "A Europe that Protects: Countering Hybrid Threats", https://eeas.europa.eu/topics/economic-relations-connectivity-innovation/46393/europe-protects-countering-hybrid-threats_en accessed 27 July 2020 , 2020

4 Europol, *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, 2020

5 Wolford, Ben, "Does the GDPR apply to companies outside the EU?", https://gdpr.eu/companies-outside-of-europe/, 2020

6 Palmer, Danny, "GDPR: 160,000 data breaches reported already, so expect the big fines to follow" https://www.zdnet.com/article/gdpr-160000-data-breaches-reported-already-so-expect-the-big-fines-to-follow/, 2020

7 Schwab, Pierre-Nicolas, "European GDPR statistics: evolution of the number of complaints per country", https://www.intotheminds.com/blog/en/gdpr-statistics-europe/ , 2019

8 Verizon, *2020 Data Breach Investigations Report*, 2020

9 Many interviewees used the term sophistication in connection to a variety of threats. The widespread use of the term, however, also makes its value as a descriptor limited. Certain sources aim to further unravel the answer to what makes a particular tactic or modus operandi sophisticated. See DePaula, Nic & Sanjay Goel, "A Sophistication Index for Evaluating Security Breaches", *11th Annual Symposium on Information Assurance*, 2016, and Buchanan, Ben, "The Legend of Sophistication in Cyber Operations", https://www.belfercenter.org/publication/legend-sophistication-cyber-operations, 2017

10 Europol, *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, 2020

11 See IIJ America, "Allow / Deny List (Domain Policy Set Level)", https://iijasd.zendesk.com/hc/en-us/articles/206289805-Allow-Deny-List-Domain-Policy-Set-Level-, 2015 and the UK National Cyber Security Centre, "Terminology: it's not black and white", https://www.ncsc.gov.uk/blog-post/terminology-its-not-black-and-white, 2020

12 Chainalysis, "The Chainalysis Crypto Crime Report is Here. Download to Learn Why 2019 Was the Year of the Ponzi Scheme", https://blog.chainalysis.com/reports/cryptocurrency-crime-2020-report, 2020

13 Paquet-Clouston et al., "Spams meet Cryptocurrencies: Sextortion in the Bitcoin Ecosystem", *Advances in Financial Technology (AFT19)*, https://arxiv.org/pdf/1908.01051.pdf , 2019

14 BBC, Coincheck: World's biggest ever digital currency 'theft', https://www.bbc.com/news/world-asia-42845505, 2018

15 At the time of writing – August 2020.

16 European Commission, "February infringements package: key decisions", https://ec.europa.eu/commission/presscorner/detail/en/inf_20_202 , 2020

17 Coin ATM Radar, https://coinatmradar.com/, 2020

18 European Commission, "Protecting victims' rights", https://ec.europa.eu/info/policies/justice-and-fundamental-rights/criminal-justice/protecting-victims-rights_en#:~:text=The%20European%20Commission%20presented%20on,fully%20rely%20on%20their%20rights, 2020

19 See for example https://twitter.com/EC3Europol activities.

20 For more information see Europol and Eurojust's reports on the Observatory Function.

21 Alrwais, Sumayah et al., *Under the Shadow of Sunshine: Understanding and Detecting Bulletproof Hosting on Legitimate Service Provider*, IEEE Symposium on Security and Privacy, 2017

22 State Criminal Police Office Rhineland-Palat-

inate, https://www.presseportal.de/blaulicht/pm/29763/4387169, 2019

23 Chainalysis, "Ransomware Attackers Aren't Sparing Anyone During Covid-19", https://blog.chainalysis.com/reports/ransomware-covid-19 , 2020. Also see BBC News, "NHS 'could have prevented' WannaCry ransomware attack", https://www.bbc.com/news/technology-41753022, 2017, and Winder, Davey, "Infection Hits French Hospital Like It's 2017 As Ransomware Cripples 6,000 Computers", https://www.forbes.com/sites/davey-winder/2019/11/20/infection-hits-french-hospital-like-its-2017-as-ransomware-cripples-6000-computers/#5db5ae55576e, 2019

24 Krebs, Brian, "REvil Ransomware Gang Starts Auctioning Victim Data", https://krebsonsecurity.com/2020/06/revil-ransomware-gang-starts-auctioning-victim-data/, 2020

25 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2018*, 2018

26 Krebs, Brian, "REvil Ransomware Gang Starts Auctioning Victim Data", https://krebsonsecurity.com/2020/06/revil-ransomware-gang-starts-auctioning-victim-data/, 2020

27 Goodin, Dan, "LockBit Is the New Ransomware for Hire", https://www.wired.com/story/lockbit-is-the-new-ransomware-for-hire/, 2020

28 Virsec, "Maze & Other Ransomware Groups Say They Won't Attack Hospitals During COVID-19 Outbreak-But How Trustworthy Is Their Word?", https://virsec.com/maze-and-other-ransomware-groups-say-they-wont-attack-hospitals-during-covid19-outbreak-but-how-trustworthy-is-their-word/, 2020

29 Hammersmith Medicines Research, "HMR targeted by cyber criminals", https://www.hmrlondon.com/hmr-targeted-by-cyber-criminals, 2020

30 Intel 471, "Understanding the relationship between Emotet, Ryuk and Trickbot", https://blog.intel471.com/2020/04/14/understanding-the-relationship-between-emotet-ryuk-and-trickbot/, 2020

31 AWS Shield, "Threat Landscape Report – Q1 2020", https://aws-shield-tlr.s3.amazonaws.com/2020-Q1_AWS_Shield_TLR.pdf, 2020

32 European Commission, "Preventing and Combating Child Sexual Abuse and Exploitation: Towards an EU Response", https://audiovisual.ec.europa.eu/en/video/I-191928, 2020

33 Canadian Centre for Child Protection, "International Survivors' Survey", https://protectchildren.ca/en/programs-and-initiatives/survivors-survey/, 2017

34 Europol, "Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic", https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic, 2020

35 Canadian Centre for Child Protection, "International Survivors' Survey", https://protectchildren.ca/en/programs-and-initiatives/survivors-survey/, 2017

36 Europol, "Partners & Agreements – Police2Peer: Targeting file sharing of child sexual abuse material", https://www.europol.europa.eu/partners-agreements/police2peer, 2020

37 Europol, "Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic", https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic, 2020

38 BBC News, "NSPCC urges Facebook to stop encryption plans", https://www.bbc.com/news/technology-51391301, 2020 and Musil, Steven, "Facebook urged to halt encryption push over child abuse concerns", https://www.cnet.com/news/facebook-urged-to-halt-encryption-push-over-child-abuse-concerns/, 2020

39 Europol, "International police cooperation leads to arrest of Darkweb child sex abuser in Spain", https://www.europol.europa.eu/newsroom/news/international-police-cooperation-leads-to-arrest-of-dark-web-child-sex-abuser-in-spain, 2020

40 Europol, "Operation CHEMOSH: how encrypted chat groups exchanged Emoji 'stickers' of child sexual abuse", https://www.europol.europa.eu/newsroom/news/operation-chemosh-how-encrypted-chat-groups-exchanged-emoji-%E2%80%98stickers%E2%80%99-of-child-sexual-abuse, 2020

41 Europol, "Exploiting isolation: offenders and victims of online child sexual abuse during the COVID-19 pandemic", https://www.europol.europa.eu/publications-documents/exploiting-isolation-offenders-and-victims-of-online-child-sexual-abuse-during-covid-19-pandemic, 2020

42 Wongsamuth, Nanchanok, "Online child sexual abuse cases triple under lockdown in Philippines", https://news.trust.org/item/20200529090040-3ejzo/ , 2020

43 Europol, "90 suspects identified in major online child sexual abuse operation", https://www.europol.europa.eu/newsroom/news/90-suspects-identified-in-major-online-child-sexual-abuse-operation, 2020

44 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2019*, 2019

45 Europol, "COVID-19: Child Sexual Exploitation", https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation, 2020

46 Europol, "COVID-19: Child Sexual Exploitation", https://www.europol.europa.eu/covid-19/covid-19-child-sexual-exploitation, 2020

47 Europol, "The SIM hijackers: How criminals are stealing millions by highjacking phone numbers", https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers, 2020

48 Europol, "The SIM hijackers: How criminals are stealing millions by highjacking phone numbers", https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers, 2020

49 Cimpanu, Catalin, "FBI: BEC scams accounted for half of the cyber-crime losses in 2019", https://www.zdnet.com/article/fbi-bec-scams-accounted-for-half-of-the-cyber-crime-losses-in-2019/, 2020.

50 Stupp, Catherine, "Fraudsters Used AI to Mimic CEO's Voice in Unusual Cybercrime Case", https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402, 2019

51 Krebs, Brian, "Wawa Breach May Have Compromised More Than 30 Million Payment Cards", https://krebsonsecurity.com/tag/jokers-stash/, 2020

52 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

53 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2019*, 2019

54 Digital Shadows, "Darkweb Search Engine Kilos: Tipping the Scales In Favor of Cybercrime", https://www.digitalshadows.com/blog-and-research/dark-web-search-engine-kilos/ , 2020

55 Digital Shadows, "Darkweb Search Engine Kilos: Tipping the Scales In Favor of Cybercrime", https://www.digitalshadows.com/blog-and-research/dark-web-search-engine-kilos/ , 2020

56 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

57 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

58 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

59 Europol, "Darkweb child abuse: administrator of Darkscandals arrested in the Netherlands", https://www.europol.europa.eu/newsroom/news/dark-web-child-abuse-administrator-of-darkscandals-arrested-in-netherlands, 2020

60 Europol, *Catching the virus: cybercrime, disinformation and the COVID-19 pandemic*, 2020

61 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020

62 Fuentes, Mayra Rosario, "*Shifts in Underground Markets: Past, Present, and Future*", 2020