
EUROPOL
INTERNET ORGANISED CRIME THREAT ASSESSMENT 2021

Internet Organised Crime Threat Assessment (IOCTA) 2021

Luxembourg: Publications Office of the European Union, 2021

PDF ISBN: 978-92-95220-35-5 ISSN: 2363-1627 doi:10.2813/113799 QL-AL-21-001-EN-N

Cite this publication: Europol (2021), Internet Organised Crime Threat Assessment (IOCTA) 2021, Publications Office of the European Union, Luxembourg.

Your feedback matters.

By clicking on the following link or scanning the embedded QR code you can fill in a short user survey on the received strategic report.

Your input will help us further improve our products.

https://ec.europa.eu/eusurvey/runner/eus_strategic_reports

Contents

Foreword

Catherine De Bolle
EXECUTIVE DIRECTOR OF EUROPOL

I am pleased to introduce the Internet Organised Crime Threat Assessment (IOCTA) 2021.

The IOCTA is Europol's flagship strategic product that provides a law enforcement-focused assessment of evolving threats and key developments in the area of cybercrime. We are grateful for the many contributions from our colleagues in European law enforcement and private sector partners that make this report possible. Combining law enforcement and private sector insights allows us to present this comprehensive overview of the threat landscape.

In this year's report, the impact of the COVID-19 pandemic remains visible. Cybercriminals have continued exploiting opportunities created by lockdowns and continued teleworking. Ransomware affiliate programs have increased in prominence and are tied to a multitude of high-profile attacks against healthcare institutions and services providers. Mobile malware operators and fraudsters have leveraged the increased reliance on online shopping services and are increasingly using it as a part of their *modi operandi* to access their victims' bank accounts. Children spending more time online has made them more susceptible to grooming, leading to an increase of self-produced exploitation material.

Many of the threats in the cybercrime landscape are exacerbated by the growing crime-as-a-service market on the Dark Web. Malware-as-a-service offerings and the auctioning of people's stolen data enable the planning of future attacks. Criminals also continue improving their operational security by abusing end-to-end encrypted communication services and cryptocurrencies.

Europol continues to be at the forefront of law enforcement innovation and offers various policing solutions in relation to encryption, cryptocurrencies and other challenges. We have continued to provide reliable support to high-profile cross-border operations against cyber threats, with an increase from 57 operations in 2013 to 430 in 2020.

We will continue to support the international law enforcement community by fostering an effective legal and regulatory framework for investigating cyber threats, and by supporting the training of future cyber-investigators.

Abbreviations

AaaS Access-as-a-Service

AI Artificial intelligence

AML Anti-money laundering

ATM Automated teller machine

ATS Automated Transfer System

APT Advanced persistent threat

BEC Business email compromise

BPH Bulletproof hosting

CEO Chief executive officer

CIS Commonwealth of Independent States

CNP Card not present

CSAM Child sexual abuse material

CSE Child sexual exploitation

CSIRT Cyber Security Incident Response Team

C2 Command and control

DDoS Distributed Denial of Service

DGA Domain generation algorithm

E-commerce Electronic commerce

EC3 Europol's European Cybercrime Centre

EU MS European Union Member States

E-skimming Electronic skimming

IOCTA Internet Organised Crime Threat Assessment

IP Internet protocol

ISP Internet service provider

IT Information technology

KYC Know your customer

LDCA Live distant child abuse

MaaS Malware-as-a-Service

NIS Network and information security

NGO Non-governmental organisation

OpSec Operational security

OTP One-time password

PGP Pretty Good Privacy

P2P Peer-to-peer

RaaS Ransomware-as-a-Service

RAT Remote access trojan

RDP Remote desktop protocol

SIM Subscriber identity module

VoIP Voice over Internet Protocol

VPN Virtual private network

2FA Two-factor authentication

Executive summary

The central theme of last year's IOCTA was that cybercrime is an evolution not a revolution. While that still holds true, the past 12 months have been a testament to the fact that exceptional circumstances accelerate that evolution. The new reality that the global pandemic has brought forth requires rapid adaptation and it is likely that the pace and organisation of personal and professional life has been permanently transformed. Inevitably, these developments have also spurred innovation among cybercriminals as they have strived to capitalise on new opportunities.

Ransomware groups, which continue to be a key threat, have been increasingly taking advantage of widespread teleworking by scanning potential targets' networks for insecure remote desktop protocol (RDP) connections and keeping a keen eye on disclosed virtual private network (VPN) vulnerabilities. Mobile malware operators have leveraged the increase in online shopping by using delivery services as phishing lures to trick their victims into downloading their malicious code, stealing their credentials or perpetrating different forms of delivery fraud. Mobile banking trojans have become a specifically noteworthy threat due to the increased popularity of mobile banking. Criminals have continued utilising COVID-19 narratives for the online sale of counterfeit medical products and vishing to steal login credentials. There are also reports that distributed denial of service (DDoS) attacks for ransom might be making a comeback due to an increased reliance on online services. During lockdowns, children spend an even larger part of their day online, which has led to a steep increase in online grooming. Minors are now more likely to self-produce and share explicit material for online reputation or monetary gain or due to coercion.

In addition to being successfully opportunistic, threat actors have continued to mature in their methods and organisation. Cybercriminals continue to move towards a more calculated target selection and there is a rise in ransomware affiliate programs seeking cooperation with hackers and other malware developers. Ransomware operations are becoming increasingly focused on high-value attacks on large organisations and their supply chains while social engineers are shifting their attention towards upper-level management. These trends were highlighted in the previous IOCTA, but the transition has been quicker than many might have anticipated, with numerous large-scale intrusions like those of Microsoft Exchange Server, SolarWinds and Kaseya coming to light in the past 12 months.

Perpetrators continue to be increasingly ruthless and methodical in their *modi operandi.* Last year Europol wrote about the rise of ransomware crews deploying double-extortion methods by exfiltrating victims' data and threatening to publish it. In the past 12 months, the arsenal of coercion methods has expanded with cold-calling journalists, victims' clients, business partners and employees. In addition, many of the most notorious ransomware affiliate programs deploy DDoS attacks against their victims to pressure them into complying with the ransom demand.

These *modi operandi* are becoming more popular with criminals conducting investment fraud as well, which European law enforcement reported as one of the key threats. Those organising these schemes are setting up local call centres to increase their credibility with different language-speaking victims, as well as re-targeting their 'customers'. Once a person has realised that their investments have been stolen, fraudsters contact them again under the pretext of representing law firms or law enforcement agencies, offering to help retrieve their funds.

In light of these developments, the market for criminal goods and services is booming. Personal information and credentials are in high demand as they are instrumental in improving the success rate of all types of social engineering attacks. Unfortunately, the market in personal information flourishes as ransomware and mobile information stealers produce an abundance of marketable material as a by-product of the primary attack. It is also not a coincidence that Malware-as-a-Service (MaaS) offerings have increased, with ransomware affiliate programs leading the charge.

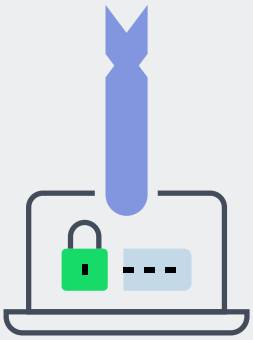
Although Bitcoin currently remains the go-to cryptocurrency of choice for Dark Web users and vendors, Monero and other privacy coins are rising in popularity. Criminals are increasingly converting their illicit earnings made in Bitcoin using cryptocurrency obfuscation methods like swapping services, mixers and coinjoins. Child sexual abuse material (CSAM) is actively traded on peer-to-peer (P2P) networks and the Dark Web, where cryptocurrencies are also used for payments, with law enforcement reporting an increase in for-profit distribution.

With all these opportunities, the administrators of online criminal markets have not remained idle. The increase in law enforcement activity in the past few years has incentivised them to enhance their operational security to protect their profits. They have established new mechanisms for protection against DDoS attacks from competitors and prefer hosting their services in countries where international judicial cooperation for law enforcement is more challenging. Additionally, many platforms have stopped automating their Pretty Good Privacy (PGP) encryption to prevent the decryption of exchanged messages in case the authorities seize the market. Illegal markets have expanded to different encrypted communication channels due to increased legal action taken by law enforcement. These include channels like Telegram and Wickr.

It is apparent that digitisation affects all forms of criminality. Methods and tools used by cybercriminals are increasingly adopted in other crime areas and the digital criminal ecosystem continues to evolve at an alarming pace. The privacy and convenience offered by communication, distribution and cryptocurrency platforms are beneficial in all illegal activity. Online anonymity is exacerbated by the wide-scale adoption of encryption technologies, which can benefit lawful users and criminals simultaneously, creating a paradoxical situation for policymakers. In addition to legitimate services, international law enforcement is keeping a keen eye on VPN and crypto phone providers that cater to the criminal elements of our society.

To combat the aforementioned advancing threats, law enforcement officers need to be able to have timely access to data and to conduct lawful undercover work to keep society safe. Companies, especially those operating outside the European Union, have to improve their Know Your Customer (KYC) and information disclosure practices. Law enforcement agencies need more training and tools to have officers capable of uncovering and disrupting criminal activity in the digital realm. Finally, it is vital to continue improving our collective information technology (IT) literacy and awareness as cybercrime has become entrenched in our society.

Key findings



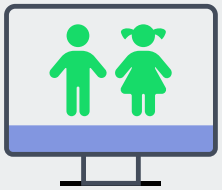
Cyber-dependent crime

* Ransomware affiliate programs are using supply-chain attacks to compromise the networks of large corporations and public institutions and utilise new multi-layered extortion methods.

* Mobile malware has become a scalable business model by introducing overlay attacks, two-factor authentication disruption and SMS-spamming capabilities

* DDoS for ransom seems to be making a return as criminals use the names of well-known advanced persistent threat (APT) groups to scare their targets into complying with ransom demands.

Child sexual exploitation material



* There has been a steep increase in online grooming activities on social media and online gaming platforms.

* The production of self-generated material is a key threat. This material is displaying increasingly younger children.

* Overall activity related to child sexual abuse material (CSAM) distribution on P2P networks has increased considerably.

* The Dark Web remains an important platform for the exchange of CSAM.

Online fraud

* COVID-19 continues to have a significant impact on the European fraud landscape in the second year of the pandemic.

* Phishing and social engineering remain the main vectors for payment fraud, increasing in both volume and sophistication.

* Investment fraud is thriving as citizens incur devastating losses, but business email compromise (BEC) and CEO fraud also remain key threats;

* Card-not-present fraud appears under control as COVID-19 restrictions curb travel-based types of fraud.

Dark Web

* Dark Web users are increasingly using Wickr and Telegram as communication channels or to bypass market fees.

* Dark Web users are increasingly adopting anonymous cryptocurrencies, such as Monero, and swapping services.

* Users rely on increasingly sophisticated operational security, migrating quickly to other (userless) markets or markets enforcing manual PGP after takedowns.

* Grey infrastructure is increasingly helping Dark Web users thrive.

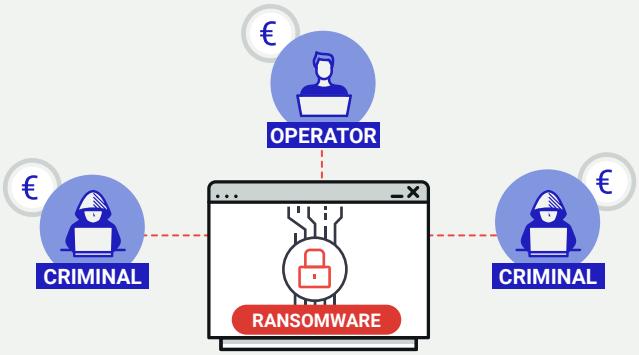
Introduction

In previous versions of the IOCTA it was highlighted that the persistent nature of various *modi operandi* meant that changes of cybercrime threats were rarer than commonly perceived. Last year's IOCTA captured the landscape by reflecting on how cybercrime is an evolution rather than a revolution. This year's IOCTA, therefore, aims to have a more restricted focus on changes and developments that have taken place during the last 12 months. This means the document is more focused and limits its discussion on cybercrime threats. The aim is to highlight that, in the absence of fundamental changes, we still have to recognise the rapidly evolving nature of cybercrime.

Despite our intended focus on new or adapted *modi operandi*, we also emphasise that we need to take into consideration the persistence of certain cybercrime threats. Methods that still prove fruitful for perpetrators of cybercrime merit our continuous attention, since only through dedicated and joint efforts will these perpetrators and their methods become less successful.

For this year's IOCTA, the project team surveyed all European Union Member States (EU MS), a limited number of third countries[1], members of Europol's advisory groups[2] and internal specialists. These were asked about what changes had specifically taken place in the threat landscape over the past 12 months. By limiting ourselves to four questions[3] about the past 12 months, focused on changes in the prevalence and *modi operandi* of cybercrime, we wanted to ensure that our approach focused on the most relevant developments. The inclusion of input from trusted partners in the private sector through our Advisory Group members also assisted in the development of a comprehensive overview of the most up-to-date cybercrime threat landscape.

The fight against ransomware



RANSOMWARE AFFILIATE PROGRAMS

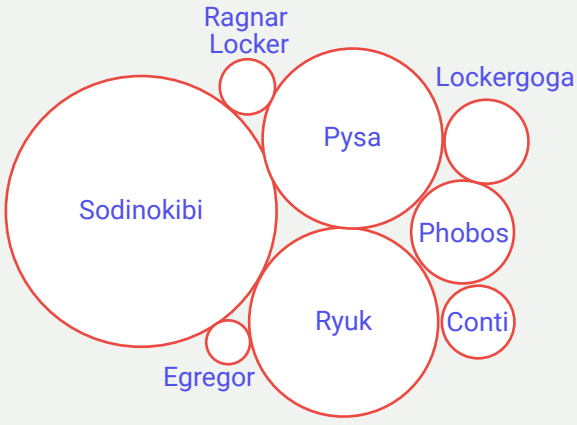
Calling clients, employees, business partners and/or journalists to pressure victim

Threatening DDoS attack against victim

Exfiltrating data and threatening publication/action

WHAT EUROPOL IS DOING

RANSOMWARE CASE REQUESTS TO EUROPOL
2020 - 2021



EUROPEAN MALWARE ANALYSIS SOLUTION (EMAS)
Contributions increase 2020 - 2021
100%

EMPACT
Cybercrime – Attacks Against Information Systems

J-CAT
JOINT CYBERCRIME ACTION TASKFORCE
Coordinated action against key cybercrime threats and targets

NO MORE RANSOM
Provides the victims of ransomware tools to decrypt their systems

WHAT OTHERS ARE DOING

WEF'S 'PARTNERSHIP AGAINST CYBERCRIME EFFORT TOWARDS COMBATTING RANSOMWARE'

This initiative is the bundling of forces of various private parties within the World Economic Forum. It focuses on active disruption approaches, supporting law enforcement efforts, and policy adjustments to hinder ransomware success.

STOPRANSOMWARE INITIATIVE (US)

The StopRansomware Initiative consolidates ransomware resources from federal government agencies and includes prevention advice, targeting audiences such as small businesses with information for protecting their networks.

RANSOMWARE TASK FORCE (US)

A public private effort which provides the following priority recommendations:

- directing nation states away from providing safe havens for ransomware criminals;
- 'a sustained, aggressive, whole of government, intelligence-driven anti-ransomware campaign';
- Cyber Response and Recovery Funds, mandate reporting, and require organisations to consider alternatives to paying;
- closer regulation of the cryptocurrency sector.

EUROPOL RECOMMENDS

STRONGER FOCUS ON PREVENTION

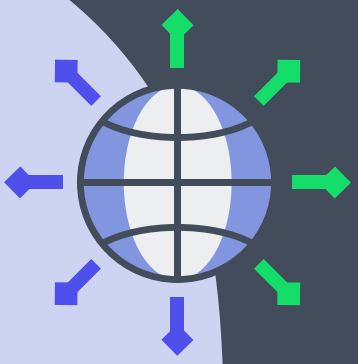
- National governments should make businesses of all sizes aware of the risks of falling victim to ransomware and offer practical guidelines in securing their networks.

ENHANCE INSIGHT INTO RANSOMWARE ATTACKS TO FACILITATE EFFECTIVENESS OF CRIMINAL INVESTIGATION

- Increase law enforcement coordination via international initiatives such as J-CAT;
- Encourage reporting to law enforcement by victims of ransomware attacks.

TARGET GREY INFRASTRUCTURE FACILITATING RANSOMWARE CRIMINALS

- Target bulletproof hosters;
- Impose KYC and AML requirements for cryptocurrency exchanges globally.



1

Cross-cutting crime and challenges

The continued increase of cyber- and computer-related crime is to a large degree enabled through the evolution and maturation of the criminal markets that provide all the necessary tools, goods and services to novice and established criminals. Network intrusions and social engineering are components of a multitude of attack vectors.

Criminals are increasing their operational security by hiding their online activity, using more secure communication channels and obfuscating the movement of illicit funds. The universality of these practices creates monetary incentives for the expansion of both the crime-as-a-service business model and grey infrastructure.

1.1 Crime-as-a-service continues to proliferate

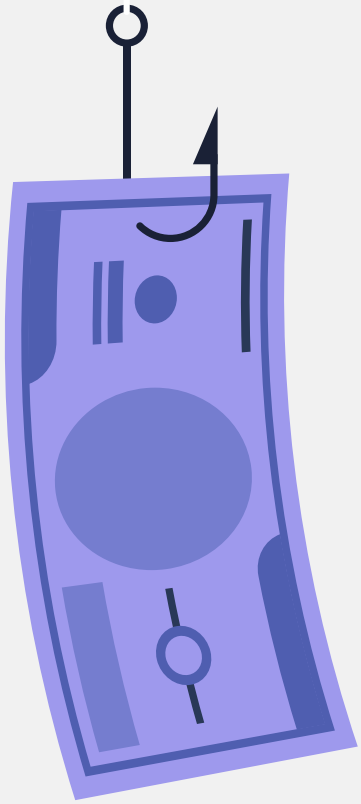
The crime-as-a-service (CaaS) model remains a prominent feature of the cybercriminal underground and is a cross-cutting factor throughout the cybercrime sub-areas. The availability of exploit kits and other services not only serves criminals with low technical skills[4], but also makes the operations of mature and organised threat actors more efficient.

In the past 12 months, European law enforcement agencies have reported an increase in MaaS offerings on the Dark Web, of which ransomware affiliate programs seem to be the most prominent. These programs are an evolution of the Ransomware-as-a-Service (RaaS) model in which the operators share profits with partners who can breach a target network and either harvest all the information required to launch an attack or deploy the malware themselves. This has expanded the market of selling access to compromised infrastructure and data breaches.

Related to the activities of ransomware and mobile malware operators, access-as-a-service (AaaS) is also in high demand as it is an enabler for both advanced malware crews and low-level criminals renting the tools to access corporate networks.

The by-product of the rise of multi-layered extortion schemes and wide-scale mobile information theft campaigns is an influx of personal information to illegal markets. This type of data is sought after by a wide range of offenders as it can drastically improve the success rate of social engineering deployed in any form of attack. As it stands, the user is often still the weakest link in the IT-security framework, which means social engineering remains an important vector for acquiring access to an information system or, in cases of fraud, the victim's bank account.

One of the challenges related to the ongoing evolution of the market for criminal services is the planning of investigatory resources. Most often, the offenders actually causing harm to the victims are end users of criminal services. This means that investigations against these individuals are rather low-impact in terms of the disruption to the criminal ecosystem. Although all the available tools must be utilised to arrest the perpetrators, this needs to be done in parallel to internationally coordinated actions against the key players who are running the platforms and services that enable these crimes in the first place.



1.2 Expansive use of grey infrastructure enhances criminals' operational security

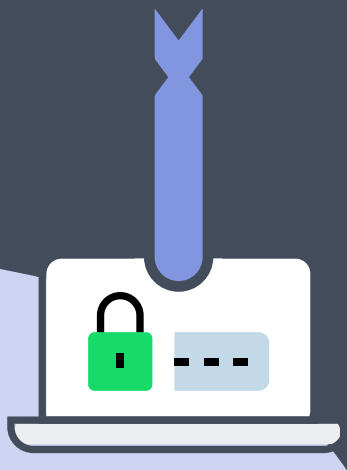
Besides CaaS, various other services, tools and technologies continue to help facilitate cybercrime[5]. Some of these are legitimate services that are widely used, but are inadvertently useful for achieving the goals of cybercriminals: secure communication, anonymity, obfuscation and laundering of criminal proceeds, and more. Other services can be classified as operating in a 'grey' area. Such services are often located in countries with very strong privacy laws or a history of not cooperating with the international law enforcement community. These are used by criminals and advertised in criminal forums. Grey infrastructure services include bulletproof hosters, rogue cryptocurrency exchanges, and VPNs that provide safe havens for criminals.

Legitimate services that are abused by cybercriminals are commonplace. The most well-known feature of such services is strong end-to-end encryption. Messaging application providers are unable to disclose the contents of the messages exchanged on their service even when subpoenaed. The amount of (meta)data stored on users is very limited[6].

Other legitimate tools and techniques that are abused by cybercriminals include cryptocurrencies and VPNs. Cybercriminals obfuscate and launder illicitly earned funds via cryptocurrencies. Fortunately, many legitimate cryptocurrency exchanges have strengthened their know-your-customer (KYC) regulations since the introduction of guidelines and directives at various levels[7]. Unfortunately, cryptocurrency laundering remains possible through the persistence of mixers, swapping services and exchanges operating in grey areas (see section 5.5). Cybercriminals may also use legitimate VPN providers, as these will provide them with a safe and secure browsing experience. These companies will still comply with lawful requests for information when their services are abused for cybercriminal activity. European law enforcement, however, increasingly focuses on services that do not simply operate to give users a secure experience, but rather optimally shield cybercriminals from the grasp of law enforcement. Some recent examples include the takedowns of ANOM, Sky ECC, EncroChat, and several VPNs and cryptocurrency mixers.

These services are the grey infrastructure that makes cybercriminals thrive: they services abuse jurisdictions with lagging legislation for hosting, do not store user data in a sufficient manner, and/or do not comply with lawful requests. Although not all users of such services are necessarily criminals, the level of criminality associated with such services is often so high that national law enforcement agencies, after finding enough evidence of criminal abuse, could consider them to be criminal enterprises.

During the last year, Europol has – together with its partners – coordinated takedowns of various services operating in grey areas, such as the takedowns of two VPNs that provided safe havens for cybercriminals: DoubleVPN[8] and Safe-Inet.[9] In addition, the takedowns of encrypted communication providers (also known as 'crypto phones') have led to the arrests of hundreds of criminals and the seizure of tons of illegal drugs, firearms, and millions of euros. However, more importantly, these operations have provided global law enforcement agencies with invaluable insights into the operations of criminals and their networks.



2

Cyber-dependent crime

During the last 12 months, a number of developments pertaining to the dominant threats within the cyber-dependent crime threat landscape have emerged. Malware operators, especially those associated with ransomware affiliate programs, have improved their attack *modi operandi* and their malware functionalities. Mobile banking trojans have made a break-through thanks to the increasing number of users preferring to conduct their financial activities via mobile devices. Criminals also seem to have realised the increased impact that DDoS attacks have on their targets' systems if there is a lack of physical alternatives, which has brought about a re-emergence of financially motivated DDoS attacks.

Key Findings

- Ransomware affiliate programs are using supply-chain attacks to compromise the networks of large corporations and public institutions, and utilise new multi-layered extortion methods.
- Mobile malware has become a scalable business model by introducing overlay attacks, two-factor authentication disruption and SMS-spamming capabilities.
- DDoS for ransom seems to be making a return as criminals use the names of well-known advanced persistent threat (APT) groups to scare their targets into complying with ransom demands.

2.1 Ransomware continues to dominate and proliferate

Although the world has changed drastically over the last 12 months, one constant that has remained is the threat that ransomware poses to our financial, public and even physical safety. A majority of law enforcement respondents noted that ransomware reports had increased during the reporting period. The trends of focusing on large corporations and public institutions, utilising vulnerabilities in the digital supply chain, and multi-layered extortion that we observed last year have intensified and become more prominent, which is an indication of the increased sophistication and maturation of the ransomware affiliate programs involved.

Attackers focus on high-value targets

The use of traditional mass-distributed ransomware seems to be in decline and perpetrators are moving towards human-operated ransomware targeted at private companies, the healthcare and education sectors, critical infrastructure and governmental institutions. The shift in the attack paradigm indicates that ransomware operators choose their targets based on their financial capability to comply with higher ransom demands and their need to be able to resume their operations as quickly as possible. Conti, Maze, Avaddon and Babuk are a few examples of ransomware groups engaged in targeting large corporations, while Ryuk ransomware is notorious for being widely used in attacks specifically against the healthcare system.

This seems to indicate that spending more time on large corporations and public institutions is an effective approach for cybercriminals in terms of the return on investment. However, threat actors have started to consider law enforcement attention drawn to their operation to be an important criterion in their internal cost-benefit analysis. Some ransomware affiliate programs have started changing their policies to restrict their partners from attacking certain targets. For example, DarkSide stated that it would introduce moderation after the Colonial Pipeline attack drew global attention, Avaddon ransomware has built in features to avoid targets in the Commonwealth of Independent States (CIS), and Sodinokibi (also known as REvil) has prohibited attacks on the social and governmental services of any country.

Increase in opportunities and sophistication

Since the beginning of the pandemic, cybercriminals have been taking advantage of the fact that most companies have had to at least partially resort to teleworking, which meant that IT security policies have become more relaxed and the overall number of vulnerabilities and attack surfaces have increased. In

particular, the large number of remotely connected unmanaged endpoints has continued to be an opportunity for criminals throughout this year as well. Threat actors have continued penetrating organisations' networks through remote desktop protocol (RDP) connections and exploiting vulnerabilities in VPN services. They pay close attention to recently disclosed vulnerabilities, such as the Pulse Connect Secure VPN flaws, and utilise scanning tools to locate unpatched servers belonging to a potentially desirable target.

The previous IOCTA reported on the potential threat that attacks can pose on IT supply chains. During the reporting period, we have seen these concerns come to fruition through the examples of the SolarWinds, Kaseya and Microsoft Exchange Server attacks. Criminals have realised how much potential there is to compromise digital supply chains – organisations need to grant network access to update distributors, which makes these third-party service providers an ideal target. After infiltrating a software provider's client network, ransomware operators can choose the most suitable targets, traverse their network further under the disguise of legitimate users, and then deploy their malicious code at the most opportune time. Furthermore, IT-infrastructures are extremely intertwined, so a successful intrusion does not only put one company's clients at risk, but potentially also opens doors to compromise other service providers, giving the attack even greater scalability.

Ransomware attacks have become more sophisticated as criminals spend more time inside the network researching the target and escalating their privileges in order to further compromise the infrastructure and get their hands on more data. Criminals use tools like Metasploit, Cobalt Strike and Mimikatz in their post-exploitation framework for lateral movement inside the network. Additionally, threat actors have started utilising fileless malware (using a system's native tools to execute a cyber-attack) more extensively to avoid common detection methods that scan for malicious file attachments or the creation of new files. Fileless ransomware attacks use native scripting languages to write malicious code directly into the target system's memory, or hijack built-in tools like PowerShell to encrypt files.

Extra layers of extortion added

In 2020, we reported the rise of double-extortion methods, whereby criminals deploying ransomware used data exfiltration and the threat of publishing it as added pressure on their targets to comply with their ransom demands. European law enforcement agencies and Europol have identified several new extortion methods that cybercriminals use to pressure their victims.

Ransomware crews have started using Voice over Internet Protocol (VoIP) services to call journalists, the organisation's clients and business partners for further coercion. In some cases, ransomware operators also threaten their victims with DDoS attacks and the publication of their employees' personal information if they do not comply with the ransom demand. Some of the more infamous ransomware groups utilising these tactics are Avaddon, DarkSide, RagnarLocker and Sodinokibi.

Due to more strategic targeting, the greater time spent before executing attacks, and multi-layered extortion methods, private partners have reported a sharp rise in the number of ransom payments made (over 300% increase)[10] between 2019 and 2020, with

known transactions totalling over USD 400 million. Additionally, the average paid ransom amount increased from USD 115 123 in 2019 to USD 312 493 in 2020 (over 170% increase)[11].

Rise of the ransomware affiliate programs

All the extra time and effort put into ransomware attacks for a bigger pay-out is enabled by the continuous development and specialisation of the criminal services ecosystem (Crime-as-a-Service model). Over the past year, a rise was identified in ransomware affiliate programs, whether sold publicly to a wide range of potential users or offered privately to a smaller group of hackers.

Public ransomware affiliate programs are not an entirely new phenomenon, as actors breaching a victim's system and then paying a RaaS operator to use their malware has been an observed dynamic in the cybercriminal ecosystem for quite some time. More cause for concern comes from the rise of private affiliate programs that are usually operated by better-known criminal ransomware groups, such as Conti, DarkSide, Sodinokibi/REvil, NetWalker and Babuk. These threat actors are seeking out developers and hackers to improve the functionality of the malware or gain access to high-value targets' infrastructure.

Ransomware crews are also collaborating with other malware developers. One such example is how perpetrators used EMOTET to deliver ransomware payloads to target networks[12]. Since its disruption in January 2021, other modular malware variants like BazarLoader and IcedID have started replacing EMOTET. There have been reports that Ryuk ransomware, which was previously also distributed via the EMOTET botnet, was deployed to victims' systems after a TrickBot infection, which might suggest a partnership between the two groups. These trends are indicative of the fact that ransomware attacks will continue to evolve and increase in magnitude.

EMOTET takedown

In January 2021, law enforcement and judicial authorities worldwide took down the Emotet botnet.

Emotet opened doors for:

Trickbot, QakBot and Ryuk were among the malware families to use Emotet to enter a machine.

How did Emotet work?

Luring the victims

Emotet was delivered to the victims' computers via emails that contained a malicious link or an infected document.

Installation

If victims opened the attachment or the link, the malware got installed.

Infection

The computer became vulnerable and was offered for hire to other criminals to install other types of malware.

2.2 Mobile malware threat becomes reality

Mobile malware has been a looming threat in Europe for a long time, but has never materialised to the extent expected due to the lack of scalability as a sustainable business model. Unfortunately, cybercriminals have made a breakthrough this year, and the number of mobile malware reports to law enforcement has increased significantly.

Mobile banking trojans improved

The Android banking trojan threat landscape now includes new tactics and techniques for stealing credentials. A number of mobile banking malware families have implemented new on-device capabilities to commit fraud by manipulating the banking apps on the user's device using the Automated Transfer System (ATS) modules powered by the Android Accessibility Service. Banking trojans like Cerberus and TeaBot are also capable of intercepting text messages containing one-time passcodes (OTPs) sent by financial institutions and two-factor authentication (2FA) applications such as Google Authenticator.

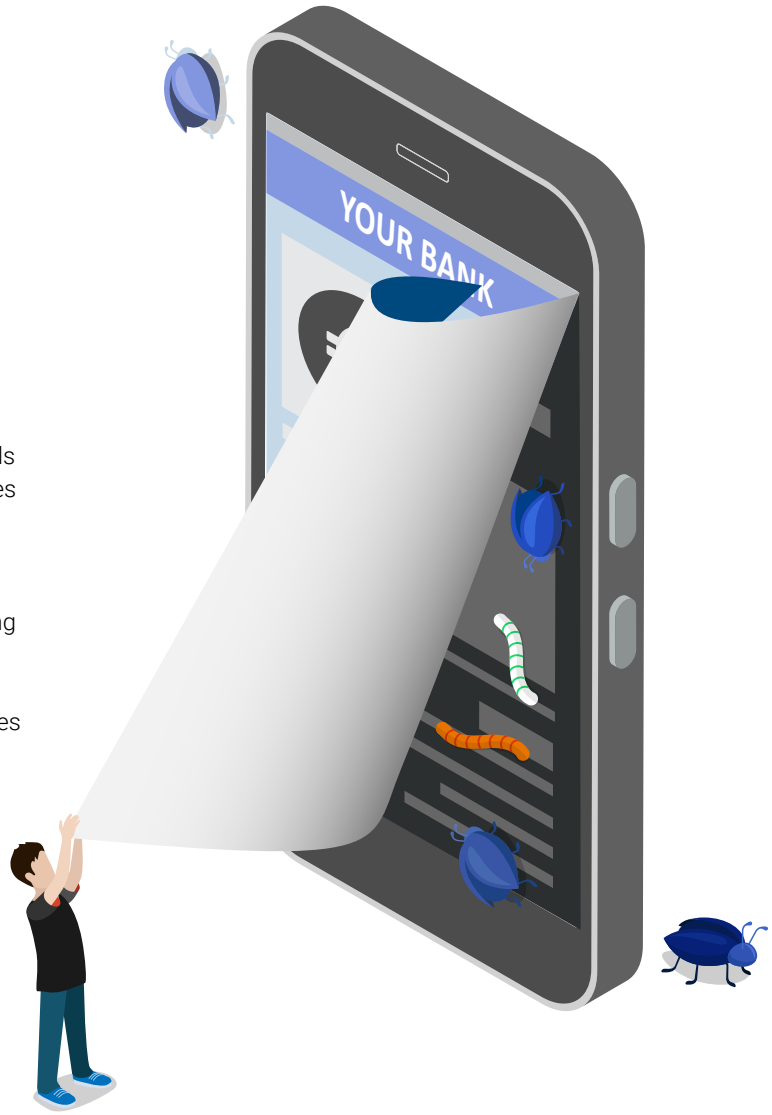
FluBot is spreading rapidly

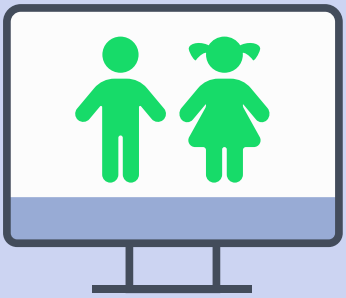
FluBot is currently one of the most prolific mobile banking trojans wreaking havoc in Europe and the United States. A key part of the malware's functionality is its ability to install display overlays for Google Play verification and various banking apps, which enables the theft of victims' credentials (banking, credit card and crypto wallet). FluBot uses a domain generation algorithm (DGA) to connect to its C2 server, generating a list of domains to try until it finds one it can reach. Using this method, threat actors can switch the domains they are using for C2 communication quickly as they become blocked or taken down. FluBot spreads through self-propagation by sending phishing text messages from the infected device to its contact list.

2.3 Monetarily incentivised DDoS attacks re-emerge

Law enforcement and private partners are reporting a re-emergence of DDoS attacks accompanied by ransom demands, as well an increase in high-volume attacks compared to the previous year. Cybercriminals have been targeting internet service providers (ISPs), financial institutions, and small and medium-sized businesses (SMBs).

Usually, a small-scale demonstration attack against the target entities' services precedes the ransom demand. The attackers have started to claim to be associated with well-known advanced persistent threat groups (APTs) like Fancy Bear and Lazarus in order to scare the victim into paying the ransom. There are mixed reports about the consequences of non-compliance, where in some cases the threat of a large-scale attack did not materialise, while in others, such as the New Zealand Stock Exchange attack, the threat actors followed through with their promise.





3

Child sexual abuse material

The main trends and threats related to online child sexual exploitation have stayed relatively stable throughout the reporting period. While a series of factors have affected the evolution of these criminal activities, law enforcement did not detect significant changes. The production and distribution of child sexual abuse material (CSAM) have been influenced by the increasing unsupervised presence of children online. The proliferation of encrypted messaging applications and social media platforms have an impact on the grooming methods and distribution of CSAM amongst offenders.

Key findings

- There has been a steep increase in online grooming activities on social media and online gaming platforms.
- The production of self-generated material is a key threat. This material is displaying increasingly younger children.
- Overall activity related to CSAM distribution on P2P networks has increased considerably.
- The Dark Web remains an important platform for the exchange of child sexual abuse material (CSAM).

3.1 The production and dissemination of child sexual abuse material remains a major concern

The production and dissemination of CSAM online have been major concerns since the inception of the Web. Law enforcement agencies and non-profit organisations engaged in child protection detect an overwhelming amount of material every year. In many cases, perpetrators produce CSAM in the victim's domestic environment, most often created by those in the child's circle of trust[13].

Children are accessing the internet unsupervised at a very young age and spend long hours using electronic devices. This exposes them to substantial threats. The COVID-19 pandemic has had a significant impact on the presence of children online. National lockdowns have forced remote and virtual learning, while the inability to participate in social activities has resulted in significantly more time spent online gaming and on social media platforms. Additionally, the increasing normalisation of sexual behaviour online[14] is changing younger people's attitude to sharing explicit content with each other. These societal changes have provided offenders with a wider group of potential victims exposed to internet usage for longer periods of time in more vulnerable circumstances.

3.2 The production of self-generated material is a key threat

During the reporting period, law enforcement agencies reported a surge in the detection of self-generated material exchanged on social media, also displaying children of a younger age. NGOs engaged in the detection and removal of CSAM online report that almost two-thirds of the confirmed reports contained self-generated material, often captured in the victim's own bedroom[15]. Abusers exploit vulnerabilities to get in contact with and gain the trust of minors online before proceeding with the abuse leading to self-production by the victims. Law enforcement agencies report a peak in online grooming cases over the last year, especially on social media and gaming platforms. On other occasions, minors are having online sexual interactions with abusers who gain their trust by pretending to be their peers. Offenders using fake identities often obtain self-generated material by means of manipulation or blackmail.

The production of self-generated material is many cases a consequence of sextortion. Some research points to the production and exchange of sexual images by teens as an exploration of their sexuality[16]. However, such exchanges, even with people they know in person and believe they can trust, are problematic since the creator of the image or video loses control of it once they send it to someone else. Minors also produce material both for financial gain and to boost their

online status on particular platforms, seeking likes and other indicators of approval[17].

Some offenders move from online to offline abuse. In some cases, abusers have persuaded victims to have meetings in real life, transforming the online abuse into a physical one that can also last over time through coercion or extortion.

The European Commission is working on a proposal for an EU centre to prevent and counter child sexual abuse. Its goal is to ensure an effective and coordinated approach to child sexual abuse in the EU. It will cover prevention, support to LE and service providers, and support to victims. Europol's central role, as foreseen by the EU Commission, in the proposed EU centre for the prevention and countering of child sexual abuse, would ensure that it continued to provide high-quality services to the EU Member States and partners with operational agreements. Europol's victim-focused approach in the area of online child sexual abuse, as evidenced through the Victim Identification Taskforce and initiatives like Trace an Object – Save A Child, along with preventive initiatives such as #SayNo, positions the organisation well to take such a role.

3.3 Cases involving live distant child abuse (LDCA) continue to increase

Travel and contact restrictions prompted by the COVID-19 pandemic have likely influenced the threat of LDCA, making it a viable alternative for those who would normally be transnational child sex offenders. LDCA can be an additional source of production of CSAM. Some offenders record or capture victims performing live-streamed sexual acts for them, without the victims' knowledge. This way of producing new material is often referred to as 'capping', which comes from the phrase to capture victims' material[18]. Law enforcement agencies have observed the exchange of new 'capped' material on Dark Web forums.

3.4 Peer-to-peer (P2P) file sharing networks remain important channels for the distribution of CSAM

CSAM is usually stored online or locally on password-protected drives. Offenders often make use of end-to-end encrypted communication channels, social media platforms and image boards to share illicit content. Private groups dedicated to the exchange of CSAM continue to proliferate on messaging applications.

Peer-to-peer (P2P) file sharing networks remain an important channel for sharing CSAM from user to user or within small groups. Some countries have reported a considerable overall increase in the use of P2P distribution networks. This trend is consistent with the peak reported during the early stages of the COVID-19 pandemic[19] and later confirmed when comparing data from 2019 and 2020. P2P activity was, however, reported as decreasing in the IOCTA 2020.

3.5 The Dark Web persists as an important platform for the exchange of CSAM

Despite successful law enforcement actions in taking down platforms focused on child sexual abuse, groups facilitating the exchange of CSAM on the Dark Web keep proliferating and are a persistent threat[20].

Offenders often share illicit content in these groups through direct links to image hosts in the Clearnet and Dark Web where the CSAM is stored. In some cases, they also make use of cyberlocker sites where users pay content providers for each sign-up and subsequent download of their content[21].

Forums are well-structured and users are hierarchically organised depending on their roles. Users take up roles depending on their contribution to the community and can be administrators, moderators or users. In several cases, users take up the moderator role in several platforms, facilitating distribution of CSAM with wider audiences.

The use of these specialised platforms is not limited to the dissemination of material but opens a forum of exchange for like-minded people where offenders can share experiences, methods to commit abuse, and successful countermeasures to evade or hinder detection.

These networks are well structured, controlled and quite cohesive. New users have to gain the trust of the community in order to be accepted in the group, for example by contributing with newly created or posted CSAM. The online absence of one of the members can be a worrisome development to be flagged within the community. Affiliation rules in fact normally include active participation in the community, and inactivity may lead to loss of membership. In some cases, communities are not limited to the online dimension, with high-ranked group members also meeting in real life.

3.6 CSAM for profit continues to be a growing threat

With the exception of LDCA, offences related to child sexual abuse are not usually committed for financial gain. However, the monetisation of CSAM is a growing threat[22]. The annual revenue of CSAM sites is estimated to have more than tripled between 2017 and 2020[23]. Cryptocurrencies are the currency of choice for these types of transactions.

In some cases, offenders pay minors directly for the exchange of self-generated content. Law enforcement agencies have observed the change in the use of online platforms – which should be used by adults only for the exchange of explicit adult content – in this sense. Some of these platforms fail in preventing access by minors who register with fake identification and sell or appear in explicit videos[24].

BOYSTOWN TAKEDOWN

The Dark Web platform, known as Boystown, has been taken down by an international taskforce set up by the German Federal Criminal Police (Bundeskriminalamt) which included Europol and law enforcement agencies from the Australia, Canada, the Netherlands, Sweden and the United States[38].

This site focused on the sexual abuse of children and had 400 000 registered users when it was taken down. Several other chat sites on the Dark Web used by child sexual offenders were also seized at the same time.

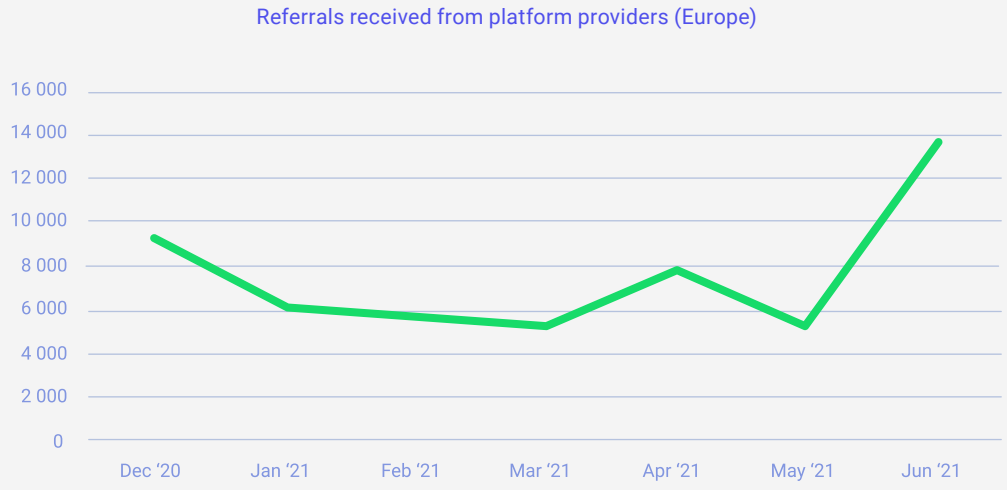
The case illustrates what Europol is seeing in child sexual abuse offending: online child offender communities on the Dark Web exhibit considerable resilience in response to law enforcement actions targeting them. Their reactions include resurrecting old communities, establishing new communities, and making strong efforts to organise and administer them.

PRIVACY and SAFETY – how to protect both

Electronic service providers play an important role in detecting, reporting and removing CSAM online. Some of these companies have been supporting the fight against online child sexual exploitation by applying specific technologies to proactively detect CSAM in their services. Detected material is then removed and referred to child protection NGOs and law enforcement agencies for analysis and investigation.

The ePrivacy Directive of 2002 aims to ensure confidentiality of communications and personal data and does not contain legal exceptions related to the detection of child sexual abuse material. Applied as such, this regulatory framework did not allow electronic service providers to continue their work in actively detecting CSAM online when the European Electronic Communications Code repealed the ePrivacy Directive in December 2020. This had a significant impact (see statistics below), considering that electronic service providers contribute the majority of CSAM reports. Additionally, due to the cross-border nature of this crime area, regional legislation has a global impact. The effect of the absence of derogations for the detection of online child sexual exploitation resulted in a 58% decrease in EU-related reports in the months following December 2020[25]. Although a temporary agreement was reached in July 2021, this is an ongoing discussion and will be reflected in the anticipated legislation to counter CSE at EU level.

It is important to safeguard citizens' privacy. It is also very important to ensure that children who are subject to child sexual exploitation online are protected by having their images detected, reported and removed from circulation on online platforms. Strict and generic regulations protecting privacy need to strongly consider child safety in their provisions.



4

Online fraud

Criminals continue making significant profits as well-known types of online fraud continue to be effective. While criminals have not had to re-invent their *modi operandi*, they continue to refine them, making them more targeted and technically advanced. Investment fraud has become a significant concern, as phishing and social engineering have further increased to generate considerable criminal proceeds. As the COVID-19 pandemic restricts travelling, the shift to online shopping has multiplied opportunities for fraud.

Key findings

- COVID-19 continues to have a significant impact on the European fraud landscape in the second year of the pandemic.
- Phishing and social engineering remain the main vectors for payment fraud, increasing in both volume and sophistication.
- Investment fraud is thriving as citizens incur devastating losses, but business email compromise (BEC) and CEO fraud also remain key threats.
- Card-not-present fraud appears under control as COVID-19 restrictions curb travel-based types of fraud.

4.1 Online shopping in times of COVID-19 leads to delivery fraud

Continuing the trend from last year, the COVID-19 pandemic has had a significant impact on the European fraud landscape. As such, European law enforcement agencies have reported an overall increase in online fraud as criminals have exploited increased online activity.

Some of these crimes make use of COVID-19-related lures, such as phishing or the sale of counterfeit medical products, while others seek to exploit the side-effects of the pandemic. These include the relaxation of established security procedures due to employees working from home and a widespread shift to online shopping.

The extension of lockdowns throughout Europe has brought with it a number of new e-commerce opportunities, which have often proven to be a target for criminals. Delivery fraud, in particular, has emerged as a new criminal focus in the second year of the pandemic. Criminals offer goods and receive payment without delivery, defraud online shops with weak security measures, or use delivery services as phishing lures. Posing as delivery services, criminals contact potential victims with links to phishing websites pretending to offer information about a parcel delivery, with the aim of obtaining user credentials and payment card details.

4.2 Criminals mix *modi operandi* as phishing and social engineering increase

The past 12 months have seen a further significant increase in phishing and social engineering. Facilitated by the ongoing pandemic, the number of COVID-19-related phishing attempts conducted above all via telephone (vishing) and text messages (smishing) has risen considerably.

While tried and tested social engineering approaches still work very well for criminals, phishing campaigns continue to evolve.

Compromised information from data breaches is easily and increasingly available. Criminals have

increasingly made use of this opportunity to improve their chances of success by creating highly targeted campaigns. Traditionally successful crimes such as business email compromise, CEO fraud, extortion and various types of scams, all profit from the availability of potential victims' personal data. As this data can be key in improving the success rate of criminal activities, this has led to a perpetual fraud cycle, in which the black market for compromised information is booming.

Vishing and smishing have particularly profited from the exploitation of stolen data. In combination with spoofing, whereby victims are contacted using legitimate-looking caller IDs or text aliases, criminals have lent these types of fraud attempts significant credibility.

In line with other developments, fraudsters more often combine traditional social engineering attempts with technical components to target especially elderly victims. The increased use of remote access trojans (RATs) in vishing, for instance, exploits a lack of technical knowledge on the part of the target, potentially leading to full account access and significant financial harm.

An emerging *modus operandi* in vishing is the safe account scam. In this type of fraud, criminals call their targets pretending to be employees of financial institutions or the police with spoofed caller IDs, informing them that they need to protect their money from criminals. To do so, they are instructed to transfer their funds to a 'safe account', which is under the control of the criminals and subsequently used in a network of money mules to launder the illicit proceeds. As with other vishing scams, the safe account scam often targets specific victims with the help of compromised information.

bank phishing emails

Phishing refers to fraudulent emails that trick the receivers into sharing their personal, financial or security information.

THESE EMAILS:

may **look** identical to the types of correspondence that actual banks send.

ask you to download an attached document or click on a link.

replicate the logos, layout and tone of real emails.

use language that transmits a sense of urgency.

In light of the COVID-19 pandemic, criminals have used vishing to gain access to victims' bank accounts in countries in which medical services are linked to mobile bank IDs. In these cases, criminals contact citizens over the phone and ask them to identify themselves for the purpose of arranging a vaccination appointment or other medical services. Criminals have exploited this circumstance to convince victims to provide their identity documents to log into bank accounts and unknowingly transfer money to the criminals.

With smishing, criminals have employed a diverse mix of *modi operandi*, contacting victims through text messages to request information, redirect to phishing websites, or distribute malware. The Classiscam (see below) and Flubot (see 2.2) campaigns demonstrate this versatility. On the other hand, SIM swapping appears to have stabilised throughout Europe, in part due to technical mitigation measures and the move away from text-based two-factor authentication. Still, some countries have seen a sharp increase, as criminals have further refined their approach and often profited from new data leaks.

A notable example of this development is the Classiscam scheme. Classiscam is an automated scam-as-a-service that propagates via Telegram and WhatsApp bots, providing fraudsters with pre-made pages intended to steal banking information from customers. Classiscam initially focused on delivery services, and subsequently expanded to online marketplaces and classifieds.

4.3 Investment fraud, BEC and CEO fraud cause devastating losses

The top threats in the area of non-cash payment fraud relate to investment fraud, business email compromise and CEO fraud, as criminals further refine and improve their ***modi operandi***.

Investment fraud has emerged as the most dominant type of fraud in the last 12 months. While last year put this type of crime on the map properly for the first time, criminals have continued to target victims with fraudulent investment opportunities. With different assets on offer, cryptocurrencies emerged as the most popular, as the price surge earlier in 2021 attracted a number of new investors. Fake investment websites are particularly suited in this context, since criminals can exploit lack of knowledge and, in some jurisdictions, regulatory hurdles regarding access to cryptocurrency exchanges.

At the same time, criminals are further refining and improving this type of fraud. Authentic-looking advertising campaigns, the illicit use of celebrities, and even personal recommendations through online dating schemes all help bring unsuspecting victims to these fake platforms. In addition, criminals are becoming more professional, running local call centres to target different languages, creating more legitimate-looking websites, using remote access software to take over victims' accounts, and operating complex money mule networks.

This mixing up of different *modi operandi* is a key trend in investment fraud. Increasingly, criminals are hitting their victims twice: following the theft of the investments, criminals contact the victims pretending to be lawyers or law enforcement agents offering help to retrieve their funds. With the help of spoofing and detailed knowledge about the theft, they are often able to defraud their victims several times.

Investment fraud poses a significant challenge for law enforcement. The use of cryptocurrencies means that perpetrators can launder criminal proceeds quickly and efficiently, while uncooperative exchanges, or those with weak KYC measures, make them difficult to identify. At the same time, fake investment websites do not directly target legitimate financial institutions, but abuse their brands to target members of the public, leading to a decreased incentive for the industry to take action. Since many victims have incurred significant losses – in some cases entire life savings – investment fraud is a serious type of crime with potentially devastating consequences.

As investment fraud takes the spotlight, business email compromise (BEC) and CEO fraud have remained key threats in the past 12 months, with some countries reporting a further increase in the number of cases. Continuing to lead to significant losses, both types of crime have grown in sophistication and become more targeted. Heavily relying on social engineering, attacks have increasingly focused on upper-level management, as well as on impersonating other staff members or changing invoice data in commercial transactions.

4.4 Card-not-present fraud under control as travel restrictions curb ATM attacks

Card-not-present (CNP) fraud appears to be largely under control. In countries that did see an increase in CNP cases, criminals often made use of the circumstances of the COVID-19 pandemic. Food delivery services, gaming platforms and other e-commerce platforms were targets of fraud or were exploited to steal card data.

While this data was previously centrally available at Joker's Stash, the closing of this Dark Web marketplace saw the emergence of many smaller card shops in its place. Some of its most active successors are Entershop, Trump's Dumps and Fe-Shop.

The shift from physical shopping to e-commerce has further led to an increased criminal focus on e-skimming. As more and more transactions are taking place through online shops, there has been an increase in the use of online skimming for the purpose of stealing card data. While the ***modi operandi*** have not changed, criminals have added a number of new e-skimmers, particularly JS sniffers, to their arsenals.

Automated teller machine (ATM) logical attacks significantly decreased when hard lockdowns were imposed in many EU Member States. This development is mainly due to the COVID-19 restrictions preventing criminals from travelling. As logical attacks on ATMs faded, criminals with technical abilities moved towards other digital attack surfaces, such as mobile devices. The drop in ATM attacks was not a permanent trend, however. As soon as lockdowns and travel restrictions were relaxed, many EU Member States started reporting a significant increase in this type of crime.

ATMs continue to be an attractive target for criminals. Many old ATM models are vulnerable to attack, as they are not updated with the latest software upgrades. Itinerant and crime-as-a-service groups are linked to black box attacks. These attacks are carried out by connecting remotely operated (e.g. via TeamViewer) external devices to ATMs. In the second stage, suspects move via wire transfers or cryptocurrency transactions.

Operation **SECRETO**

Cross-border operation coordinated by Europol and led by the Spanish National Police (Policía Nacional) and the US Secret Service.

The criminal network deceived 50 financial institutions through shell companies.

104
arrests

19
European arrest warrants executed

14
high-end vehicles seized

88
house searches

€406 000
seized in cash

+ €12 million
in damages

87 accounts
> €1.3 million frozen

5

Dark Web

With regard to the Dark Web, EU law enforcement agencies have reported few major changes in the threat landscape. While the infrastructure of Dark Web marketplaces has not changed drastically, several smaller developments that had already been taking place for some years have now become more commonplace.

Key findings

- Dark Web users are increasingly using Wickr and Telegram as communication channels or to bypass market fees.
- Dark Web users are increasingly adopting anonymous cryptocurrencies, such as Monero, and swapping services.
- Users rely on increasingly sophisticated operational security, migrating quickly to other (userless) markets or markets enforcing manual PGP, after takedowns.
- Grey infrastructure is increasingly helping Dark Web users thrive.

5.1 Criminals further strengthen operational security

Recent years have shown many successful international collaborative takedowns of Dark Web markets. This has led to a very volatile environment. Still, some vendors and markets continue to thrive. Vendors and other users of Dark Web markets, including in the field of child sexual exploitation, simply migrate to a new platform after a successful law enforcement takedown on the Dark Web. EU law enforcement have cited the increasing operational security (OpSec) of vendors and marketplaces as a growing concern. Examples of increased sophistication of markets are the mechanisms that administrators have put in place to protect Dark Web platforms against DDoS attacks, and domain hosting in countries in which cooperation with EU Member States may be difficult. Administrators of platforms even cooperate in some cases by protecting their marketplaces against DDoS attacks and by making user guides on how to operate on the Dark Web. Furthermore, vendors may be increasingly aware of the forensic techniques used by law enforcement agencies to identify them, and try to protect themselves accordingly. The availability of free penetration testing services for vendors, to see how secure their operational security is, exemplifies this awareness.

Many markets have stopped automating PGP encryption on their platform because of previous law enforcement successes in intercepting and decrypting PGP messages in the back end of seized Dark Web marketplace servers[26]. In this way, market administrators are trying to make users more aware of their encryption measures, which conversely could be a complicating factor for some non-technical users.

5.2 Similar goods and services, but more extortion and novel weapons

The types of goods and services for sale on the Dark Web have remained largely the same in the past 12 months. However, the presence of ransomware groups on dedicated hidden services on the Dark Web offering their malware 'as-a-service' has increased.

In last year's IOCTA, Europol included the development of perpetrators threatening to sell or wipe data encrypted in a ransomware attack. Several countries reported that the exposure of data of individuals and companies had gained further traction as a business

model for ransomware groups on the Dark Web. Governments have expressed similar warnings about such advanced extortion concerning ransomware groups that not only encrypted data, but also threatened to use DDoS attacks and leak stolen data if ransoms were not paid[27], as already mentioned in section 2.1.

Weapons appear to be traded increasingly on encrypted chat applications, such as Telegram and Wickr, but sold slightly less on Dark Web marketplaces. Europol assisted in the arrest of an Italian national suspected of hiring a hitman on the Dark Web[28]. Furthermore, several EU law enforcement agencies mentioned hitmen being ordered and weapons purchased on the Dark Web being seized. Several similar cases were reported in the media. For example, in the Netherlands a person was sentenced to 8 years' imprisonment for several attempts to order a contract killing via platforms on the Dark Web and encrypted chat applications[29]. Furthermore, weapons were being sold on a Dark Web marketplace taken down in May 2021 by French authorities[30]. In September 2020, an illegal workshop for printing three-dimensional weapons was dismantled in Spain, revealing a novel ***modus operandi***[31]. The suspect downloaded templates for weapons printing from the Dark Web. During one of the house searches in the joint operation by the Spanish Tax Agency and National Police, law enforcement agents encountered various 3D printers, one of which was in the process of printing a small firearm.

Furthermore, vendors have not stopped seizing the opportunity to abuse the uncertainty surrounding the pandemic by offering fake vaccines and masks for sale, consequently scamming buyers.

5.3 Fragmentation and displacement of Dark Web users

EU law enforcement identified the threat of fragmentation on the Dark Web, which is visible in various ***modi operandi***. EU law enforcement reported a further increase in single vendor shops and smaller markets on Tor and indicated that fragmentation was also visible in criminal networks, as these tend to employ various accounts on various marketplaces. Also, for example, the usage of encrypted communication platforms outside of Dark Web marketplaces for the sale of illicit goods and services has increased. Specifically, law enforcement mentioned Wickr and Telegram several times. For example, one country indicated that 70% of vendors that appeared to operate from the country of the respondent, listed on their Dark Web market profile a Wickr user name, while 20% listed Telegram contact info. This increasing usage of mainstream platforms with strong encryption, which are mostly used for legitimate purposes, poses a challenge for law enforcement agencies. It also shows the need for Dark Web investigators to broaden their focus on other platforms.

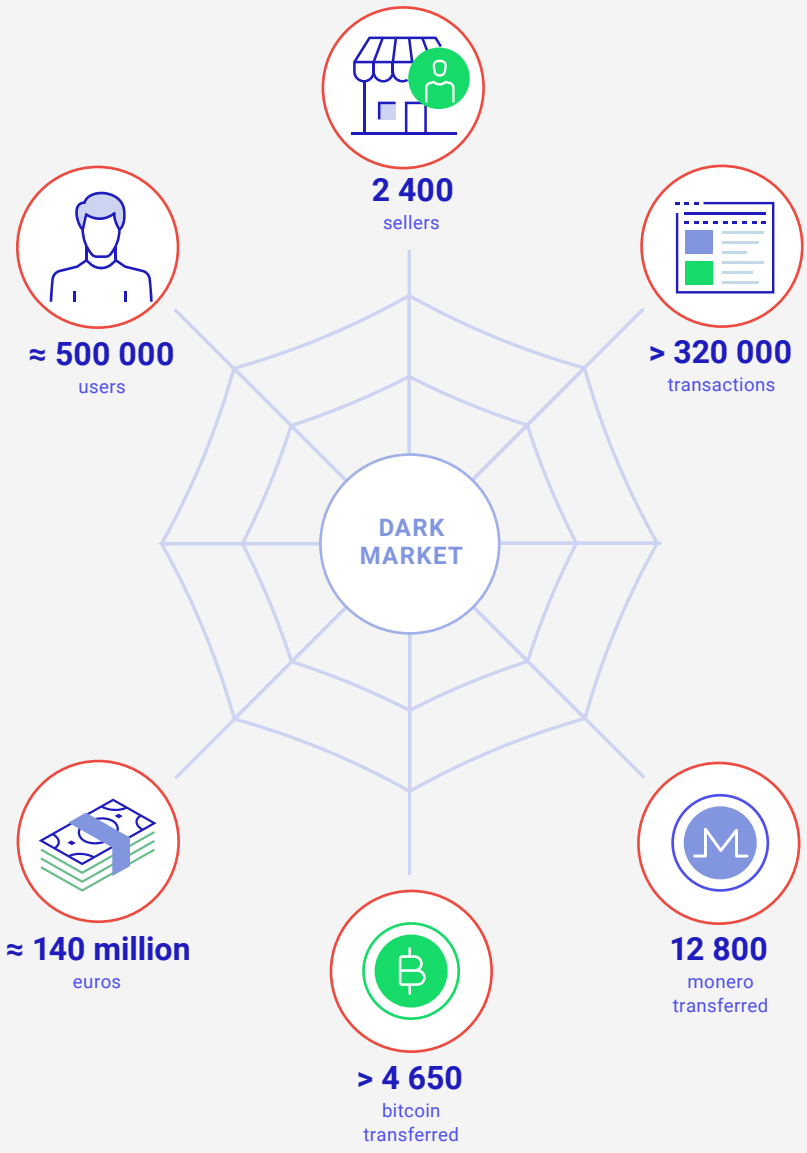
In some countries, takedowns of Dark Web marketplaces with a local or national focus may have led to this partial displacement to mobile applications[32]. Law enforcement identified the Telegram bot platform/service Televend as well as a new method of supplying or managing illicit goods locally, including for established Dark Web vendors. Televend automates part of the selling and purchasing process, but also incorporates fewer security mechanisms, which makes it more likely for users to be scammed[33]. German law enforcement have already led a successful operation, shutting down nine Telegram groups on which illegal goods and services were sold, showing that this new phenomenon is also not exempt from law enforcement intervention[34].

5.4 More use of Monero and non-cooperative swapping services

Bitcoin has by far remained the go-to cryptocurrency of choice for users of the Dark Web. However, the criminal usage of privacy coin Monero on Dark Web marketplaces has further increased. As reported last year, Monero is becoming the most established privacy coin on the Dark Web. For example, a marketplace that only accepts Monero as a payment option was around from early 2019 to October 2021. Zcash was also seen as a payment option, but its usage has not come close to Monero. While criminals still make most payments in Bitcoin, recipients are increasingly converting them to Monero and other currencies by using swapping services. These services often operate on the Clearnet and in a grey area, utilising jurisdictions with lenient legislation and vague or non-existent know-your-customer (KYC) procedures. Some other services, such as Kilos[35], are

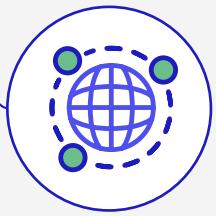
DARKMARKET

DarkMarket was perhaps the most notable takedown of a Dark Web marketplace over the last year[39].



It was the world's largest illegal marketplace on the Dark Web at the time.

The two main administrators and moderators were arrested, while the market and its criminal infrastructure was taken down in a coordinated action in collaboration between Europol and authorities in Australia, Denmark, Germany, Moldova, Ukraine, the United Kingdom and the United States.



DISRUPTOR

The coordinated operation DisrupTor showed that a Dark Web marketplace takedown not only signalled the successful ending of one investigation, but could also be the start of many others. In DisrupTor, the data gathered during the takedown of Wall Street Market was used to identify and arrest 179 vendors across Europe and the United States. DisrupTor was led by the German Federal Criminal Police (Bundeskriminalamt), with the support of the Dutch National Police (Politie), Europol, Eurojust and various US government agencies. Collaborative operations such as DisrupTor highlight law enforcement's ability to counter the encryption and anonymity of cybercriminals on the Dark Web.

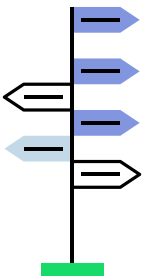
operating on the Dark Web and even admit to 'skirting legal procedures'. Kilos was already mentioned in last year's IOCTA, but now it also deploys its own swapper and mixer, called 'KSwap' and 'Krumble' respectively.

The use of swappers falls within a bigger trend of adopting more complex money laundering methods. In the early days of Dark Web marketplaces, vendors often simply transferred cryptocurrency directly from a marketplace to an exchange. However, in the last few years, many different obfuscation methods have gained popularity, such as mixers, CoinJoin, swapping, crypto debit cards, Bitcoin ATMs, local trade and more.

5.5 Grey facilitating infrastructure helps criminals thrive

The continuous thriving of cybercriminals can in part be attributed to the fact that grey infrastructure still facilitates them in many ways, as identified in the section on cross-cutting crime facilitators. This includes converting cryptocurrencies to exchanges with lacking KYC policies in place, bulletproof hosters that do not store useful client information, and the fact that grey infrastructure can operate (on paper) in countries where regulations are less stringent than in the EU. Whereas cryptocurrency exchanges operating in the EU are now regulated through the 5th Anti-Money Laundering Directive[36], this is not the case globally. In the field of bulletproof hosting there are many legal difficulties, and as such, companies will often host both legitimate and illegal content and may claim not to know about content on their servers.

Recommendations

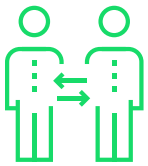


6.1 Remove certain legal obstacles for investigators

Undercover capabilities are becoming increasingly important in cybercrime investigations. Legislative limitations make it difficult for LEAs to enter closed groups with strong access controls. This is particularly prevalent in CSE investigations, where most group affiliation rules require the submission of newly produced CSAM in order to gain access to private groups, but it is also relevant in other crime areas on the Dark Web. As cybercriminals' operational security measures are increasing in various areas, the importance of undercover activities needs to be recognised.

Legal barriers around the retention and sharing of data persist. Data is often not retained for long enough with ISPs, which can lead to a loss of potential evidence. Investigations would benefit from longer data retention, but also from faster and higher-quality data exchange with service providers. Clearer rules for registering IP addresses and domains could increase this data quality. The e-evidence directive may contribute to this.

Increased international cooperation in investigations may also shorten the waiting time in some cases, as international partners might be able to obtain information more quickly. Also, increased international cooperation, for example in blockchain analyses, could lead to deconfliction and minimise cases where multiple authorities are chasing the same leads. Still, such cooperation is not always feasible and improved legal alignments are needed.



6.2 More officers, tools and training needed

More technically skilled officers and training are needed to adequately address cybercriminality, because of the increased technical sophistication. In the field of CSE, for example, technical solutions to increase victim identification are needed. The development of cutting-edge technologies – ideally in cooperation with law enforcement – and a stronger focus on undercover activities will contribute to the goal of fighting cybercrime and enhancing victim identification. Data analysis tools, such as for cryptocurrency tracing and decryption, are of increasing importance in investigating many types of cybercrime, but are often expensive. Still, some free initiatives exist that may help investigations, such as the new decryption platform, which was inaugurated by Europol and the European Commission in December 2020[37].

6.3 A broader cooperative focus

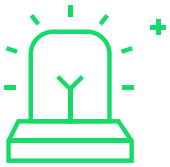
In addition to individual targets and marketplaces, law enforcement officers should broaden their focus. While these targets are important to address, those who continuously facilitate cybercriminals and their infrastructures should not remain unpunished. Examples include bulletproof hosters, criminal VPNs, illicit cryptocurrency exchangers, and money laundering platforms. Furthermore, encrypted chat applications are increasingly used by cybercriminals, demanding a broader focus from LEAs. Coordinating activities internationally can contribute to effective and timely enforcement responses. However, improvements in collaboration and task division between departments in national agencies, such as economic crime and cybercrime, should not be overlooked.

6.4 Integrate law enforcement in the cybersecurity ecosystem

Law enforcement has an essential and complementary role to play in the response to cyberattacks. Europol has been making considerable contributions to high-profile cross-border operations against cyber threats with an increase from 57 operations in 2013 to 430 in 2020. Europol wishes to highlight this in particular with regard to policy developments such as the Network and Information Security (NIS) Directive 2.0 and the introduction of a Joint Cyber Unit.

LEAs play a vital role in addressing the main gaps identified in the NIS 2.0 Impact Assessment, specifically in the joint situational awareness and joint crisis response in the event of cyber incidents of a suspected malicious nature. One of the best ways to enhance the joint situational awareness and de-conflict the actions during a cyber incident or crisis response would be to involve Europol's EC3 as observer in the relevant NIS Cooperation Group Work Streams, CSIRT Network and CyCLONe.

While the EU MS' competent NIS authorities and CSIRTs play a vital role in the response to incidents caused by system failures, third-party failures, human errors or natural phenomena, the response to incidents of a suspected malicious nature can only be comprehensive and effective if the LEAs are involved from the outset. LEAs need a victim to report the incident in order to launch an investigation and provide support. Europol recommends that it be mandatory for major cyber incidents affecting critical sectors or essential service providers of a suspected criminal nature to be reported to LEAs and EC3, just as they have to be reported to the CSIRT when it comes to other root causes. EC3 supports the cyber incident response at LEA level to all incidents of a suspected malicious nature that affect two or more EU MS, and already has established and well-functioning procedures and a collaboration framework to do so. Law enforcement agencies should be firmly embedded within the cybersecurity crisis management frameworks. The role of LEAs at national level within the national cybersecurity crisis management frameworks should be enhanced, and clear roles and responsibilities should be assigned to the competent authorities. If the LEAs and the LE response protocol were added to the international cyber incident response framework of the NIS2, they would assist the NIS competent authorities and CSIRTs by sharing expertise in complex cross-border investigations.



6.5 Streamline information sharing and enhance awareness campaigns

After receiving a legal request by a law enforcement agency, companies based outside the EU may in some cases release limited amounts of information. Such information could be more helpful to law enforcement agencies if these companies had to operate according to similar rules as in the EU. Also, standard machine-readable data would help investigators process data from such requests quicker.

Intensified public-private partnerships may contribute to the diminished success of cybercriminals. For example, expertise and information sharing with financial institutions can help to obtain data on cybercriminals and may help rapidly block their criminal proceeds. Law enforcement agencies should also explore new partnerships, such as with KYC providers, to enrich their intelligence in different areas, such as on money mules. Companies can also contribute to a decrease in fraud by increasing validation on the consumer side.

Awareness of potential victims of cybercrime should be raised at all ages, specifically in the field of child sexual exploitation where children, parents and carers should become aware of potentially risky online behaviours. Awareness campaigns on fraud with internet marketing, online investment and e-commerce fraud are also needed to help reduce fraud and prevent victimisation.

References

1 Iceland, Norway, Switzerland and the United Kingdom which are all associate members of the European Union Cybercrime Task Force (EUCTF).

2 EC3 partners: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners

3 1. *What threats have seen an increase in reporting? 2. What new and adapted MOs have you witnessed? 3. What notable cases have you had? 4. What changes do you need to be in a better position to prevent and fight cybercrime?*

4 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2020,* 2020

5 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2020,* 2020

6 These issues around encryption are extensively discussed in the recently published 'Third report of the observatory function on encryption'. See Europol, *Third report of the observatory function on encryption*, https://www.europol.europa.eu/publications-documents/third-report-of-observatory-function-encryption, 2021

7 Financial Action Task Force, *Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers*, https://www.fatf-gafi.org/publications/fatfrecommendations/documents/guidance-rba-virtual-assets.html, 2019 and Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. – Official Journal of the European Union L 156/43, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

8 Europol, 'Coordinated action cuts off access to VPN service used by ransomware groups', https://www.europol.europa.eu/newsroom/news/coordinated-action-cuts-access-to-vpn-service-used-ransomware-groups, 2021

9 Europol, 'Cybercriminals' favourite VPN taken down in global action', https://www.europol.europa.eu/newsroom/news/cybercriminals%E2%80%99-favourite-vpn-taken-down-in-global-action, 2020

10 Chainalysis, 'Ransomware 2021: Critical Mid-year Update', https://blog.chainalysis.com/reports/ransomware-update-may-2021, 2021

11 PaloAlto Networks, *2021 Unit 42 Ransomware Threat Report*, https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html, 2021

12 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2020,* 2020

13 Europol, *European Union Serious and Organised Crime Threat Assessment 2021*, 2021

14 Thorn, 'Thorn Research: Understanding sexually explicit images, self-produced by children', https://www.thorn.org/blog/thorn-research-understanding-sexually-explicit-images-self-produced-by-children/, 2020

15 The Internet Watch Foundation (IWF) confirmed 100 616 webpages displaying child sexual abuse material during the first half of 2021. Of these, 62 278 have been confirmed to contain self-generated material. See IWF, 'Campaigners push to stop this being 'the summer of online sexual abuse' against children', https://www.iwf.org.uk/news/campaigners-push-stop-being-%E2%80%98-summer-online-sexual-abuse%E2%80%99-against-children, 2021

16 Mandu, Morten Birk Hansen, 'Homosocial positionings and ambivalent participation: A qualitative analysis of young adults' non-consensual sharing and viewing of privately produced sexual images', *MedieKultur: Journal of media and communication research*, Vol. 36, No 67, https://doi.org/10.7146/mediekultur.v36i67.113976, 2020

17 Europol, *European Union Serious and Organised Crime Threat Assessment 2021*, 2021 and Internet Watch Foundation, 'Trends in Online Child Sexual Exploitation: Examining the Distribution of Captures of Live-streamed Child Sexual Abuse', https://bit.ly/2rIT0LP, 2018

18 Europol, *European Union Serious and Organised Crime Threat Assessment 2021*, 2021

19 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

20 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2020,* 2020

21 Europol, *European Union Serious and Organised Crime Threat Assessment 2021*, 2021

22 Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2020,* 2020

23 Chainalysis, *The Chainalysis 2021 Crypto Crime Report*, https://go.chainalysis.com/2021-Crypto-Crime-Report.html, 2021

24 BBC News, 'The children selling explicit videos on OnlyFans', https://www.bbc.com/news/uk-57255983, 2021

25 National Center for Missing and Exploited Children, 'A Battle Won, But Not the War in the Global Fight For Child Safety', https://www.missingkids.org/blog/2020/we-are-in-danger-of-losing-the-global-battle-for-child-safety#supportingorgs, 2020

26 Wired, 'Operation Bayonet: Inside the Sting That Hijacked an Entire Dark Web Drug Market', https://www.wired.com/story/hansa-dutch-police-sting-operation/, 2018

27 BleepingComputer, 'US and Australia warn of escalating Avaddon ransomware attacks', https://www.bleepingcomputer.com/news/security/us-and-australia-warn-of-escalating-avaddon-ransomware-attacks/ , 2021

28 Europol, 'Dark Web hitman identified through crypto-analysis', https://www.europol.europa.eu/newsroom/news/dark-web-hitman-identified-through-crypto-analysis, 2021

29 District Court of The Hague, 09/206938-20, 1 March 2021. *https://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBDHA:2021:1744*

30 French Customs, *Démantèlement du forum « Le Monde Parallèle sur le Darknet »* ('Dismantling of the 'Le Monde Parallèle' forum on the Darknet'), https://www.douane.gouv.fr/actualites/demantelement-du-forum-le-monde-parallele-sur-le-darknet, 2021

31 European Commission's European Anti-Fraud Office, 'Spain: Joint Tax Agency and National Police operation dismantled the first illegal workshop for printing 3D weapons', https://ec.europa.eu/anti-fraud/media-corner/news/04-05-2021/spain-joint-tax-agency-and-national-police-operation-dismantled-first_en, 2021

32 Examples of local Dark Web marketplaces include Flugsvamp 2.0 and Silkkittie.
See Swedish Police, 'Charges brought in extensive darknet drug trade case', https://polisen.se/aktuellt/nyheter/2020/februari/charges-brought-in-extensive-darknet-drug-trade-case/, 2020 and Europol, 'Double blow to Dark Web marketplaces', https://www.europol.europa.eu/newsroom/news/double-blow-to-dark-web-marketplaces, 2019

33 Bitcoin.com, 'A System of Robot Drug Dealers on Telegram Allows People to Buy Illegal Products for Bitcoin', https://news.bitcoin.com/a-system-of-robot-drug-dealers-on-telegram-allows-people-to-buy-illegal-products-for-bitcoin/, 2020

34 *Bundeskriminalamt*, *Illegale Marktplätze in Messengerdienst geschlossen* ('Illegal marketplaces in messenger service closed'), https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2020/Presse2020/201030_pmEVTelegram.html, 2020

35 https://www.digitalshadows.com/blog-and-research/dark-web-search-engine-kilos/

36 Directive (EU) 2018/843 of the European Parliament and of the Council of 30 May 2018 amending Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, and amending Directives 2009/138/EC and 2013/36/EU. – Official Journal of the European Union L 156/43, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018L0843

37 Europol, 'Europol and the European Commission inaugurate new decryption platform to tackle the challenge of encrypted material for law enforcement investigations', https://www.europol.europa.eu/newsroom/news/europol-and-european-commission-inaugurate-new-decryption-platform-to-tackle-challenge-of-encrypted-material-for-law-enforcement, 2020

38 Europol, '4 arrested in takedown of Dark Web child abuse platform with some half a million users', https://www.europol.europa.eu/newsroom/news/4-arrested-in-takedown-of-dark-web-child-abuse-platform-some-half-million-users, 2021

39 Europol, 'DarkMarket: World's largest illegal Dark Web marketplace taken down', https://www.europol.europa.eu/newsroom/news/darkmarket-worlds-largest-illegal-dark-web-marketplace-taken-down, 2021

This publication and more information on Europol are available on the Internet.

www.europol.europa.eu