Council of the
European Union

Brussels, 28 August 2024
(OR. en)

12867/24

COSI 136
ENFOPOL 358
CRIMORG 113
ENFOCUSTOM 103
CYBER 242

NOTE

From:	Europol
To:	Delegations
Subject:	Internet Organised Crime Threat Assessment (IOCTA) 2024

Delegations will find attached a report from Europol on the Internet Organised Crime Threat Assessment (IOCTA) for 2024, which focuses on key areas such as cryptocurrencies, cyber-attacks, child sexual exploitation and online and payment fraud schemes.


EUROPOL 25
IOCTA 2024 **
INTERNET
ORGANISED
CRIME THREAT
ASSESSMENT

EUROPOL

Internet Organised Crime Threat Assessment (IOCTA) 2024

Neither the European Union Agency for Law Enforcement Cooperation nor any person acting on behalf of the agency is responsible for the use that might be made of the following information.

© European Union Agency for Law Enforcement Cooperation, 2024

PDF ISBN: 978-92-95236-34-9 ISSN: 2363-1627 doi:10.2813/442713 QL-AL-24-001-EN-N

Reproduction is authorised provided the source is acknowledged.

For any use or reproduction of photos or other material that is not under the copyright of the European Union Agency for Law Enforcement Cooperation, permission must be sought directly from the copyright holders.

While best efforts have been made to trace and acknowledge all copyright holders, Europol would like to apologise should there have been any errors or omissions. Please do contact us if you possess any further information relating to the images published or their rights holder.

The European Union Law Enforcement Cooperation does not own the copyright in relation to the following elements:
© Vitalii Pasichnyk, on Gettyimages: pages 4-5
© Nicolas Peeters: page 6
© in-future, on Gettyimages: pages 8-9
© Nadya So, on Gettyimages: pages 10-11, 12, 17, 23, 27, 32
© Shutter2U, on Gettyimages: page 26
© dem10, , on Gettyimages: page 33
© piranka, on Gettyimages: page 35

Cite this publication: Europol (2024), Internet Organised Crime Threat Assessment (IOCTA) 2024, Publications Office of the European Union, Luxembourg.

Luxembourg: Publications Office of the European Union, 2024

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 06

Abbreviations 07

Introduction 08

Key Developments 10

1 Cryptocurrencies and the dark web: enablers of cybercrime 12

1.1 Cryptocurrencies

1.2 The dark web

2 Cyber-attacks 17

2.1 Ransomware-as-a-service

2.2 Ransomware groups

2.3 Malware-as-a-service

3 Child sexual exploitation 23

3.1 Current CSE threats

3.2 Sexual extortion and violent content online

3.3 AI-generated CSAM

4 Online and payment fraud schemes 27

4.1 Phishing

4.2 Account takeover (ATO)

4.3 Investment, BEC and romance fraud

4.4 Digital skimming attacks

4.5 ATM attacks

4.6 Online fraud and money laundering

5

Outlook: what to expect in the near future 32

5.1 AI-assisted cybercrime has only just begun

5.2 Abusing technologies

5.3 Emergence of new RaaS brands

5.4 Protecting EU payment systems

5.5 Bolstering the EU against illicit content online

5.6 The future of crypto

5.7 Renewed focus on offender prevention

References 36

Foreword

Catherine De Bolle
EXECUTIVE DIRECTOR OF EUROPOL

I am delighted to present Europol's Internet Organised Crime Threat Assessment (IOCTA) 2024, the most comprehensive yearly analysis of the latest threats posed by cybercrime in the EU. This edition marks 10 years since the release of Europol's first IOCTA. Throughout this time, the threats posed by cybercrime have evolved dynamically in terms of volume, intensity and harm potential.

The number of cybercriminals entering the market continued to grow steadily, thanks to the adoption of new technologies as well as the increasing complexity of digital infrastructures, which expands the potential attack surface.

In 2023, millions of victims across the EU were attacked and exploited online on a daily basis. Small and medium businesses were increasingly popular targets for cyber-attacks, while e-merchants experienced the most digital skimming attacks. Adults were victimised through phishing, investment and romance frauds, and more and more minors were targeted by child sexual exploitation offenders and online sexual extorters.

In parallel, a number of worldwide law enforcement actions shook the cybercriminal underground through continued arrests of ransomware affiliates and operators. Law enforcement also carried out coordinated disruption operations against cybercriminals' digital infrastructures.

Notwithstanding the growing presence of law enforcement in the dark web, this environment continues to function as an enabler for cybercrime, allowing offenders to share knowledge, tools and services in a more concealed way. In addition, the use of cryptocurrencies in a wider variety of crime areas has become more noticeable in 2023, alongside the growing number of requests for investigative support in cryptocurrency tracing received by Europol.

Cybercriminals are keen to leverage Artificial Intelligence, which is already becoming a common component in their toolbox and is very likely to see even wider application. Law enforcement agencies are expected to build a robust capacity to counter the growing threats stemming from this, both in terms of human resources and technical skills.

An additional concerning aspect of cybercrime is the young age of the offenders. As cybercriminals appear to be in many cases underage, a greater focus on offender prevention could discourage young people from entering a criminal career.



Law enforcement agencies are expected to build a robust capacity to counter the growing threats stemming from cybercriminals leveraging AI, both in terms of human resources and technical skills.



Abbreviations

2FA Two-factor Authentication
AI Artificial Intelligence
ATM Automated Teller Machine
ATO Account Takeover
BEC Business Email Compromise
BTC Bitcoin
BPH Bullet Proof Hosting
C2 Control and Command
CaaS Crime-as-a-Service
CASP Cryptocurrency Asset Service Providers
CEO Chief Executive Officer
COP Cyber Offender Prevention
CSAM Child Sexual Abuse Material
CSE Child Sexual Exploitation
DDoS Distributed Denial of Service
DNS Domain Name System
E2EE End-to-end Encryption
EBA European Banking Authority
EBF European Banking Federation
EC3 European Cybercrime Centre
EMAS Europol Malware Analysis Solution
EMMA European Money Mule Action
ESP Electronic Service Provider
ETF Exchange-Traded Fund
EU European Union
FTP File Transfer Protocol
HTTP Hyper Text Transfer Protocol
I2P Invisible Internet Project
IAB Initial Access Broker
IBAN International Bank Account Number
J-CAT Joint Cybercrime Action Taskforce
KYC Know Your Customer
LDCA Live- Distance Child Abuse
LEA Law Enforcement Agency
LLM Large Language Model
MFA Multi-Factor Authentication
MLA Mutual Legal Assistance
NFT Non-Fungible Tokens
OpSec Operational Security
OTR Off the record
P2P Peer to Peer
PI Payment Institution
PII Personal Identifiable Information
PSD3 Payment Services Directive 3
PSR Payment Services Regulation
RaaS Ransomware as a Service
RAT Remote Administration Tool
RDP Remote Desktop Protocol
SEO Search Engine Optimisation
SMB Small and Medium-sized Businesses
TCSO Transnational Child Sex Offender
USDT Tether
VOIP Voice-Over-Internet Protocol
VIDTF Victim Identification Task Force
VPN Virtual Private Network
XR Extended Reality

Introduction

In 2023, ransomware attacks, child sexual exploitation (CSE) and online fraud remained the most threatening manifestations of cybercrime in the European Union (EU). The cybercriminal landscape remained diverse, comprising both lone actors and criminal networks offering a wide range of expertise and capabilities. Some cybercriminals targeting the EU were based within the EU, while others preferred to operate from abroad, concealing their illicit operations and funds in third countries.

Continued takedowns of cybercriminal forums and marketplaces shortened the lifecycle of criminal sites, as the site administrators try to avoid drawing law enforcement (LE) attention. This uncertainty, combined with a surge in exit scams, have contributed to the continued fragmentation of criminal marketplaces. Cybercriminals' abuse of legitimate end-to-end encryption (E2EE) messaging applications also increased throughout 2023[1].

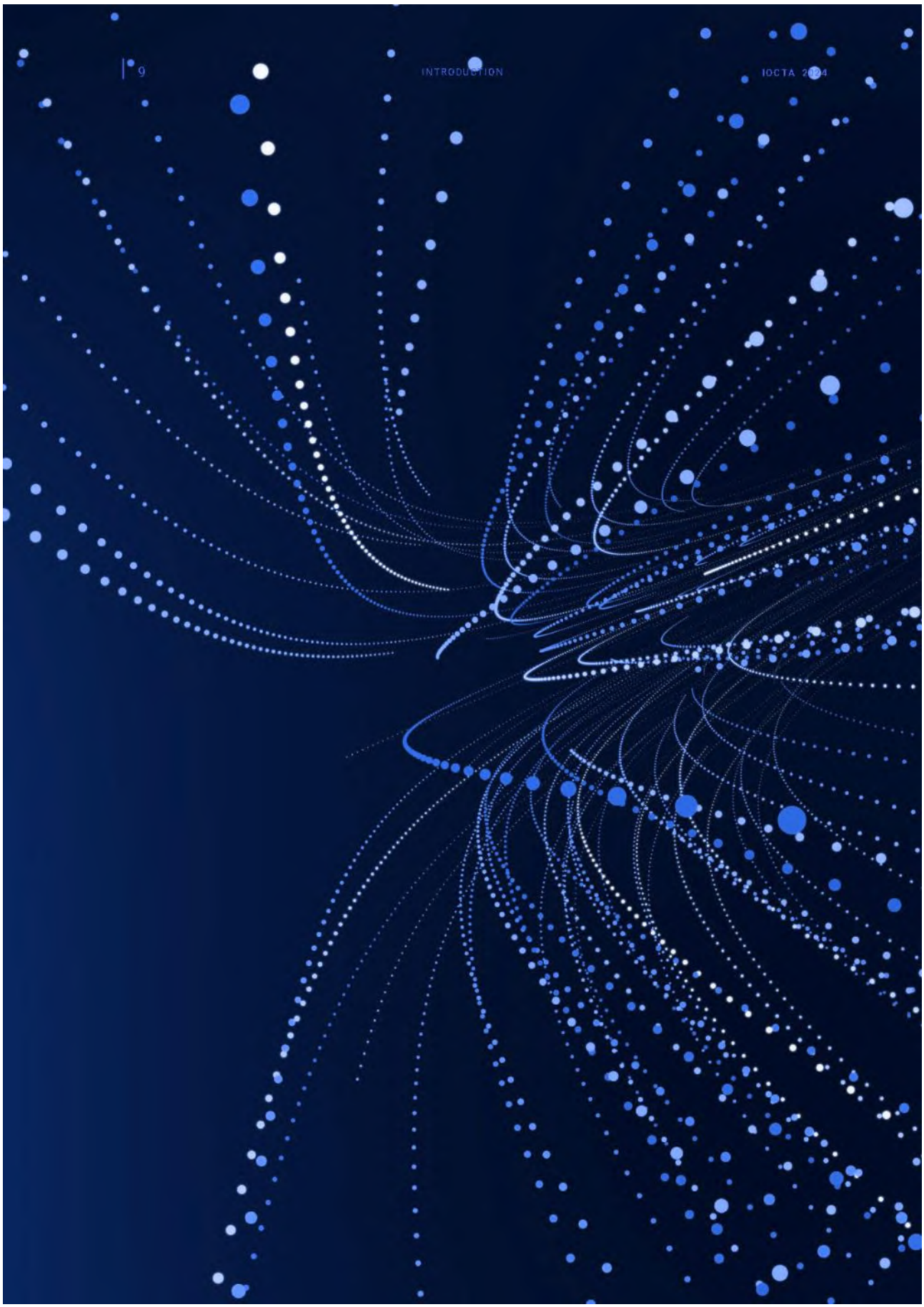
Regulatory frameworks aimed at strengthening digital systems and making the user experience more secure are being adapted, but the human factor still remains the weakest link in most cyber defence scenarios. Multi-layered extortion models are increasingly common throughout the entire spectrum of cybercrime threats. Law enforcement actions have prompted ransomware groups to disband and reorganise, making it harder to distinguish between ransomware brands and the threat actors behind the operations.

Artificial Intelligence (AI) based technologies are making social engineering even more effective.

The dynamics of the criminal market for malware and phishing services resemble the dynamics of legitimate industries, while the trade in stolen data is becoming the main threat related to crime-as-a-service (CaaS).

Malicious large language models (LLMs) are becoming prominent tools in the CaaS market. There are already services offered in the dark web that can help online fraudsters to develop scripts and create phishing emails. LLMs are also being used in sexual extortion cases, where these tools can help offenders to refine their grooming techniques.

The use of deepfakes is another area of concern as this is a powerful addition to the cybercriminal toolbox. In online fraud, deepfakes are used to mimic voices, for instance for Chief Executive Officer (CEO) fraud attempts and for shock calls, and their popularity is set to increase. In the area of child sexual exploitation (CSE), cases of AI-assisted and AI-altered child sexual abuse material (CSAM) as well as fully AI-generated CSAM were already being reported in 2023 and are expected to become more prominent in the near future.


9
INTRODUCTION
IOCTA 2024

Key developments

Main threats

- The ever-growing volume of online child sexual abuse material (CSAM) poses increasing challenges to the law enforcement (LE) community fighting online child sexual exploitation (CSE). Self-generated sexual material constitutes a significant and growing share of the CSAM that is detected online.

- Investment, business email compromise (BEC) and romance fraud remain the most common types of cyber-enabled fraud schemes in the EU, with phishing persisting as the most prevalent vector of attack. Digital skimming is an ongoing threat resulting in the theft, resale or misuse of credit card data.

- Tools and services based on AI and machine learning are becoming common tools for cybercriminals and are prominent commodities in the crime-as-a-service (CaaS) market. Beside the criminal abuse of legitimate Large Language Models (LLMs), malicious LLMs are increasingly offered on both surface and dark web, servicing offenders involved in cyber-attacks, phishing and CSE. Cases of AI-assisted, AI-altered and AI-generated CSAM have been reported and are expected to escalate in the near future. AI tools and deepfakes are also refining fraudsters' social engineering capabilities.

- As a result of worldwide LE work targeting ransomware affiliates, operators and the criminal digital infrastructure, ransomware groups have split and re-organised under different guises.

Criminal actors

- The number of cybercriminals entering the market continues to grow steadily, both due to new technologies, which effectively lower the entry barriers, and to an increasing complexity of the digital infrastructure, which widens the potential attack surface.

- The criminal landscape remains wide-ranging, comprising both lone actors and networks with various levels of expertise and capability. Some cybercriminals targeting the EU are EU-based, while others operate from abroad, concealing their illicit operations and funds in third countries.

- High-level affiliates and developers remain an important asset, with different ransomware-as-a-service (RaaS) providers competing for their services. Some affiliates are suspected of having developed their own ransomware variants to lower their dependence on RaaS providers.

Targets

- Millions of victims across the EU are attacked and exploited online on a daily basis. Ransomware groups increasingly target small and medium-sized businesses because they have lower cyber defences. E-merchants and bank institutions are the preferred victims of digital skimming attacks. Users continue to fall victim to phishing campaigns, BEC, investment and romance fraud. The number of cases of online sexual extortion targeting vulnerable minors is on the increase.

- Multi-layered extortion models are increasingly common across the whole spectrum of cybercrime threats. The illicit trade in personal data is linked due to the common occurrence of targets falling for repeated scams.

Cybercrime enablers

- The dark web continues to be a key enabler for cybercrime, allowing offenders to share knowledge, tools and services in a more concealed way. It is nevertheless unstable as the fragmentation of marketplaces continues, hand in hand with a surge in exit scams. As a result, the lifecycle of criminal sites has become shorter and mirror sites are springing up rapidly to counter takedowns. The Tor network remains the most popular platform for cybercriminals to access the dark web.

- The use of cryptocurrencies in a number of areas of crime has become more evident. Bitcoin is still the cryptocurrency that is most abused by criminals but the use of alternative coins (altcoins) seems to be growing. Underground banking for laundering crypto assets seems to be increasing, alongside the re-emergence of cryptocurrency debit cards and the regular criminal use of swapping services.

- Cybercriminal abuse of legitimate end-to-end encryption (E2EE) messaging applications keeps growing. The criminal market for ransomware, malware and phishing-as-a-service is growing and resembles the dynamics of the legitimate industry, with cybercriminals publicising their services via the dark web and E2EE.

1

Cryptocurrencies and the dark web: enablers of cybercrime

1.1 Cryptocurrencies

The criminal use of cryptocurrencies has become more evident in 2023, as has the number of requests for investigative support that Europol has received. Financial crimes, mainly investment fraud and money laundering, remains the area in which cryptocurrencies are most often encountered. Factors such as the increase in value of certain cryptocurrencies and growing media attention around crypto investments are also contributing to the steady surge in investment fraud cases.

Main types of cryptocurrencies encountered

Particularly in investment fraud, Bitcoin is increasingly being converted to stablecoins*, most likely because the latter are less subject to price volatility. Investigators encountered more of the stablecoin Tether (USDT) on the Tron blockchain compared to the Ethereum blockchain, most likely due to the low transaction fees on the Tron network. Some stablecoins have incorporated a blacklisting functionality in their smart contracts. This enables law enforcement agencies (LEAs) to request companies to freeze stablecoins that have been identified as part of a suspect's wallet.

Ransomware operators mostly ask for Bitcoin when demanding ransom, as these are still easier to obtain than other types of coins. However, there are cases where ransom demands have been made in other cryptocurrencies (e.g. Monero). The criminal use of altcoins (alternative cryptocurrencies)** seems to be increasing. The number of cases supported by Europol involving only Bitcoin were almost equal to cases that also involved altcoins.

The involvement of non-compliant services remains one of the main challenges in many cryptocurrency investigations. Whilst some companies have improved cooperation with LEAs, non-compliant services based in offshore jurisdictions often give rise to lengthy mutual legal assistance (MLA) procedures. The newly adopted EU rules on information accompanying the transfers of funds[2] – part of a package of legislative proposals to strengthen the EU's anti-money laundering and countering terrorism financing rules – have extended reporting obligations to crypto-asset service providers (CASPs). The EU rules were adopted in January 2024, and since then the European Banking Authority (EBA) has also extended its guidelines on money laundering and terrorist financing risk factors to include CASPs[3]. These developments will likely have a positive impact on the amount of information available to LEAs in cryptocurrency-related investigations, at least when suspects are located in the EU.

Crypto-money laundering

The complexity of obfuscation techniques used when laundering cryptocurrencies largely depends on the type of crime committed. Investment fraud cases involving cryptocurrencies often deploy less complex obfuscation methods, as most of it is done via traditional forms (i.e. via money mules, international bank accounts, cash movements and underground banking) rather than on the blockchain.

Groups on E2EE messaging applications seem to have replaced peer-to-peer platforms to connect people who want to exchange cryptocurrency for cash (and sometimes vice versa, e.g. cash for cryptocurrency) and avoid compliance checks. Underground banking solutions and criminal outlets to launder crypto assets also appeared to be increasing. The use of cryptocurrency debit cards has also re-emerged, as these can be used to quickly convert cryptocurrency to cash at ATMs.

In 2023, an increase in the usage of swapping services for laundering cryptocurrency was observed. Swapping is mostly done to ensure criminal funds are secure and stable – for security, cryptocurrencies are swapped to privacy coins (e.g. Monero), while for stability, cryptocurrencies are swapped to stablecoins (e.g. USDT). To comply with regulations, swapping services often provide LEAs with information on the origin, conversion and destination address.

* The term 'stablecoin' refers to a type of cryptocurrency where the value of the digital asset is supposed to be linked to a reference asset, which is either fiat money, exchange-traded commodities or another cryptocurrency. This makes it less subject to price volatility than other types of cryptocurrencies.

** The term 'altcoin' refers to any cryptocurrency other than Bitcoin. Altcoins have the same design and function, and developers can create them for various uses. The number of altcoins listed in cryptocurrency markets is rapidly multiplying, and they can be very volatile.

CRYPTOJACKER ARRESTED IN UKRAINE

In January 2024, Ukrainian law enforcement, with the support of Europol, arrested an individual believed to be the mastermind behind a sophisticated cryptojacking scheme that used compromised computers to mine cryptocurrency*. The 29-year-old hacker is thought to have been infecting the servers of a cloud provider for the purposes of cryptojacking since 2021, hacking 1 500 accounts using brute force attacks to gain passwords, before infecting the company's server equipment with the cryptojacking malware. The suspect is believed to have then created over a million virtual computers to run the malware. The whole scheme resulted in over EUR 1.8 million in mined Ethereum, Monero and TON (a cryptocurrency integrated into the user interface of Telegram). Ukrainian investigators are also looking into the suspect's potential involvement in pro-Russian hacker groups.

Europol Press Release, 12 January 2024, 'Cryptojacker arrested in Ukraine over EUR 1.8 million mining scheme',

Cyberpolice of Ukraine Press Release, 12 January 2024, 'Caused hundreds of millions of losses to the world's leading company: Cyber Police and National Police investigators exposed the hacker'

1.2 The dark web

The Tor network remains the most popular way for cybercriminals to access the dark web, despite efforts to promote the Invisible Internet Project (more commonly known as I2P) as a more LEA-proof solution.

Dark web forums are still the main channel for advertising dark web markets, although some markets also have mirrored sites on the surface web. Administrators have continued to limit the size and lifespan of their markets in order to avoid LE scrutiny, while at the same time trying to maintain a large customer base by building a good reputation via the forums. Among the reasons for the short lifespan of dark web markets are the commonly encountered 'exit scams', where administrators suddenly close a market and steal all the funds held in their escrow service. Dark web forums and chatrooms are still essential networking environments for CSE offenders to discuss CSAM and operational security (OpSec). Dark web forums for CSE offenders appear to be increasingly specialised by specific sexual preference.

Impact of recent law enforcement (LE) operations on dark web marketplaces

The increasing success rate LE is having in disrupting operations on the dark web is affecting the way dark web marketplaces are operated. The past year has seen a continued emergence of smaller and much more specialised single-vendor shops. Single-vendor shops allow vendors to avoid paying the fees imposed on traditional marketplaces for each transaction, while still maintaining a presence on several markets at the same time.

The main business in dark web markets remains illicit drugs, although there has been a noticeable rise in the volume of prescription drug sales in 2023. Fraudulent shops and services are also increasingly common, offering both fake drug sales and bogus hitman services.

* Crypto-mining is the process of validating the information in a blockchain block by generating a cryptographic solution that matches specific criteria. Once the correct solution has been found, the first miner(s) receive a reward in the form of cryptocurrencies and fees for the work done. This process also releases new cryptocurrencies in circulation.

OPERATION SPECTOR LEGACY

In the aftermath of the German LE's takedown of the Monopoly Market's criminal infrastructure in December 2021, last year saw a coordinated operation by Europol and nine countries lead to the arrest of 288 persons across nine countries suspected of involvement in buying or selling drugs on the Monopoly market. Close to EUR 51 million in cash and virtual currencies, 850 kg of drugs, and 117 firearms were seized. The vendors arrested were also active on other marketplaces.

Europol Press Release, 2 May 2023, '288 dark web vendors arrested in major marketplace seizure'

Most active cybercrime-related forums and marketplaces

Exploit, XSS and BreachForums were among the most active cybercrime forums on the dark web in 2023. Cybercriminals were seen sharing hacking knowledge and trading in stolen data, hacking tools and cybercrime services on Exploit and XSS, with the services also serving as a platform for initial access brokers (IABs). Exploit is primarily Russian-speaking and accessible via both the clear and dark web with an entry fee or a vetted reputation[4]. XSS offers security features for user anonymity and has both free and premium membership options. BreachForums is an English-language forum that functions both as a forum and a marketplace for cybercriminals globally. It facilitates the trade in leaked databases, stolen banking cards and corporate data. In May 2023, one of the forum administrators was arrested[5] and the forum was shut down. Three months later, the hacker group ShinyHunters resurrected the forum[6]. In May 2024, it was taken down again in an international LEA operation[7].

CryptBB and Dread are other known forums with increased activity in 2023. CryptBB is a closed forum for cybercriminals, including hackers, carders, and programmers, from beginners to experts (the admins of CryptBB promote it as the most suitable forum for cybercrime beginners). It offers a range of cybercrime services, remote desktop protocol (RDP) access sales, 'hackers for hire', penetration testing and bug-reporting services for marketplaces.

Dread is a forum launched in 2018 that hosts a wide variety of content from hacking to drug trafficking, Personal Identifiable Information (PII), etc. With a user base of over 400 000 users, it is considered one of the most popular forums on the dark web. The forum was shut down by a DDoS attack in November 2022 but resurrected in February 2023. It then introduced a rotating onion address service called Daunt to protect hidden services from DDoS attacks.

As for marketplaces, RAMP, Russian market and the WWH-Club were the most prolific in 2023 beside Genesis, which, although taken down in April 2023, remained one of most active markets of the year. RAMP was a prominent drug marketplace for Russian speakers between 2012, when it began, and 2017 when the Russian Ministry of Internal Affairs seized the site. In 2021, a new RAMP appeared with a focus on ransomware. The new RAMP was no longer Russian speaking only and was opened to Mandarin and English speakers. It has a closed forum with strict access criteria[8].

Russian Market is an English-language marketplace known for trading in PII and other illicit digital goods like RDP access and stolen credit card data. Despite its name, it is not directly tied to Russia or Russian speakers. The market regularly features listings of data harvested by the popular malware service RedLine Stealer*, illustrating its reliance on this malware for supplying stolen information[9]. WWH-Club is a popular Russian-language forum and marketplace known for its emphasis on cybercrime services. The forum also provides a space for discussing hacking, cybersecurity techniques and the latest cyber-threat trends.

* Redline Stealer is a malware service that first emerged in 2020 and, since then, has grown in popularity among cybercriminals. It is capable of extracting login credentials from web browsers, FTP clients, VPNs, email and messaging apps as well as collecting authentication cookies and card numbers stored in browsers, chat logs and local files. Criminals can purchase access to the platform for EUR 140 a month or pay EUR 740 for a lifetime subscription. Information gathered through this type of malware can then be used in numerous forms of cybercrime, from theft and fraud to ransomware attacks.

KKKsecforum, Viceforum, Germania, Yomi no Kuni and Kerberos were the most reported emerging forums and markets in 2023. KKKsecforum and Viceforum are mostly focused on hacking activities. Both are currently down and appear on a dark web list of breached forums. Germania is a hacking-related forum, successor to a German-speaking forum named Deutschland im Deep Web. The forum offers automated escrow in Monero for internal users, PGP authorisation and E2EE messages. Yomi no Kuni is a closed forum focusing on CSE. The Kerberos market was launched in 2022 with a clear focus on the end-user experience and security. The listings contain a wide variety of products and services ranging from drugs to digital items and stolen data. It accepts payments in both Bitcoin and Monero.

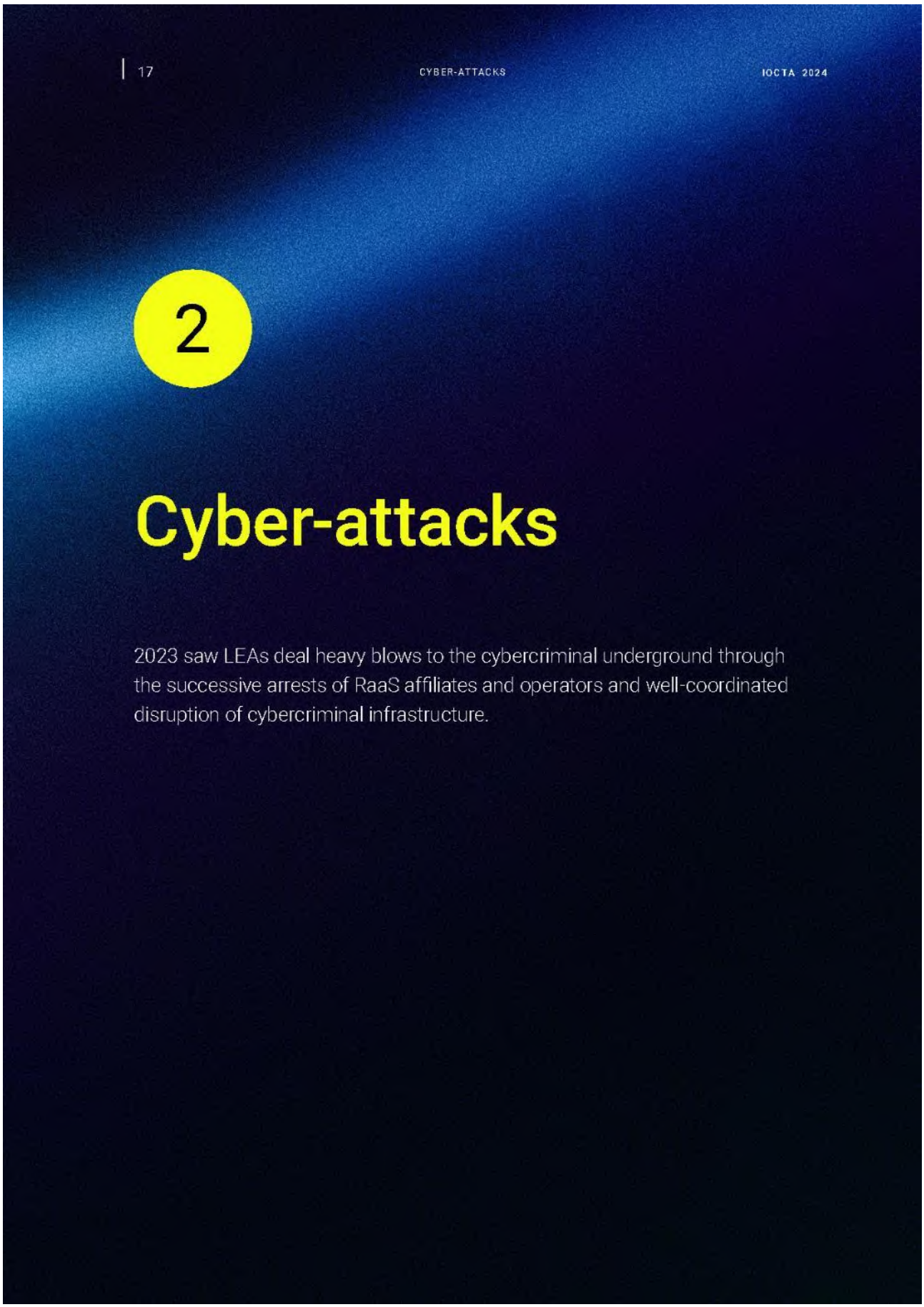
There is increased marketing of AI tools and services on the dark web. LLMs without prompt filtering are being created to help with developing and testing. The existence of a dark web service called Only Fake has already been reported. The service sells AI-generated fake IDs that can be used to open accounts online on financial services[10], bypassing Know Your Customer (KYC) procedures.

EMPACT JOINT ACTION DAYS, SOUTH EAST EUROPE 2023

From 13 to 18 November 2023, LEAs across Europe joined forces to target firearms and drug trafficking, migrant smuggling and trafficking in human beings and high-risk criminal networks during the coordinated EMPACT Joint Action Days South East Europe (EMPACT JAD SEE). In total, 26 countries from across Europe, supported by Europol, Eurojust, Frontex and INTERPOL, took part in a large-scale coordinated initiative. The cyber patrolling week focused on monitoring and investigating different websites, forums and marketplaces on the clear and dark web as well as on messaging applications and social media. Investigations were conducted in the native languages of officers from Albania, Bosnia and Herzegovina, Kosovo*, Moldova, Montenegro, North Macedonia, Serbia and Ukraine. Synchronised operations were coordinated through the JAD Coordination Centre in Skopje, North Macedonia. Investigators identified 120 targets (accounts and/or individuals) related to the trafficking of firearms, while 566 arrests were made (218 related to migrant smuggling, 186 related to drug trafficking, 69 related to firearms trafficking, and 89 related to other crimes).

Europol Press Release, 30 November 2023, '566 arrests in week of coordinated actions in Southern Europe'

* This name is without prejudice to positions on status and is in line with UNSCR 1244/1999 and the ICJ Opinion on the Kosovo declaration of independence.


2
Cyber-attacks
2023 saw LEAs deal heavy blows to the cybercriminal underground through the successive arrests of RaaS affiliates and operators and well-coordinated disruption of cybercriminal infrastructure.

Key Developments

- Ransomware groups are increasingly targeting small and medium-sized businesses because of their lower cyber defences. Target selection is also influenced by the specialisation of the Initial Access Brokers (IABs) involved in their operations.
- High-level affiliates and developers remain an important asset in the criminal underground. Different ransomware-as-a-service (RaaS) providers are competing for their services and to co-opt them into their own operations. Some affiliates are suspected of having developed their own ransomware variants to lessen their dependence on RaaS providers and their susceptibility to LE disruption.
- Recent LE operations and the leak of ransomware source codes (e.g. Conti, LockBit and HelloKitty) have led to a fragmentation of active ransomware groups and available variants. Due to their reorganisation, the distinction between ransomware brands and the threat actors behind the operations is increasingly challenging.
- LockBit was the most prolific RaaS provider on the market in 2023. Cl0p is an advanced group with access to zero-day exploits while Akira is a newcomer in the ransomware scene that might become an increasing threat.
- IcedID, Pikabot, Smokeloader, SystemBC and Danabot are some of the available and widely used alternatives to QakBot. Redline Stealer is becoming one of the go-to malware-as-a-service (MaaS) for data theft.

The ransomware landscape has become more fragmented, which is likely caused by the continued international efforts to stifle criminal groups as well as the source code leaks of Conti (2022)[11], LockBit (2023)[12] and HelloKitty (2023)[13] that have occurred in recent years. The leaked codes, combined with rapidly improving AI-tools likely facilitate an accelerated development of new ransomware variants. These factors create incentive and opportunity for ransomware groups to splinter and rebrand, not only to obstruct investigations and attribution, but also to take advantage of the chaos to grab a bigger share of the criminal market.

2.1 Ransomware-as-a-service

Ransomware groups operating under the ransomware-as-a-service (RaaS) model have tried to capitalise on the downfall of their competitors to lure capable affiliates to their service.

HIVE RANSOMWARE TAKEDOWN

In January 2023, Europol supported the German, Dutch and US authorities in taking down the infrastructure of the prolific Hive ransomware in an international operation that also involved Canada, France, Ireland, Lithuania, Norway, Portugal, Romania, Spain, Sweden and the United Kingdom. Over 1 500 companies from over 80 countries worldwide had fallen victim to Hive associates since 2021 and lost almost EUR 100 million in ransom payments. Victims were from a wide range of businesses and critical infrastructure sectors. LEAs provided the decryption key to companies that had been compromised, in order to help them decrypt their data without having to pay the ransom. Doing so has prevented about EUR 120 million in ransom payments.

Europol Press Release, 26 January 2023, 'Cybercriminals stung as HIVE infrastructure shut down'

After the disruption of Hive's services, BlackCat/ALPHV promoted their OpSec to attract affiliates previously working with Hive. One of BlackCat's selling points was that their infrastructure is hosted outside the EU and North America, in addition to having a strict no-logs policy. A similar pattern emerged after the takedown of BlackCat/ALPHV onion sites in December 2023[14], as LockBit tried to enrol their affiliates and developers. Although BlackCat/ALPHV did not immediately cease their operations, the damage done to their reputation was significant. As of March 2024, BlackCat/ALPHV seem to have shut down their operations and are suspected to have pulled an exit-scam on their affiliates[15].

LE work against ransomware operators damages the groups' reputation in the criminal underground and has an impact on their affiliates. The takedown of a ransomware service's infrastructure means that the affiliates lose access to the service, where they can generate ransomware samples and track the status of their victims. The ransomware service's back-end infrastructure can hold the personal details of the affiliates and the decryption keys for the systems they have infected. Consequently, takedowns expose affiliates to the risk of being identified and potentially cause them to lose leverage against victims. All this translates into a loss of time, effort and money spent on securing the initial access to victims' systems.

The susceptibility to LE disruption may be one of the reasons why high-level affiliates are attempting to lessen their dependence on ransomware service providers' infrastructure by utilising leaked builders to develop their own malware variants and carry out attacks more independently. This trend might also be perpetuated by the wider availability and increased quality of AI-tools that lack prompt filtering*, which cybercriminals can use to quickly assemble and debug their code.

LockBit continued to be among the most prolific RaaS providers on the market in 2023. It was taken down in February 2024 thanks to coordinated LE action involving 10 different countries, supported by Europol and Eurojust[16]. LEAs disrupted the ransomware group at every level, severely damaging their capability and credibility. Lockbit's previous popularity could be attributed to the group continuous release of new features to their platform and variants of their malware. LockBit 3.0 also known as LockBit Black, which included new obfuscation and anti-analysis features (e.g. self-deletion), was released in 2022[17]. In 2023, LockBit released LockBit Green, an updated variant of the ransomware (mainly a derivative of the leaked Conti source code) designed to target virtual computing and storage services. Additionally, the ransomware operator seemed to have also been developing encryptors for targeting MacOS devices[18].

One RaaS group that emerged at the beginning of 2023 is Akira, which threat researchers have associated with the now disbanded Conti group[19].

Considering the fast growth of Akira's victim base and their mature operational capabilities, they are likely to become an increasing threat in the near future.

* Feature used by some language models (including LLMs) to prevent the model from generating responses to prompts that contain inappropriate or harmful content.

2.2 Ransomware groups

Phobos ransomware[20], widely deployed by the 8base ransomware group, has been increasingly reported to LE. The 8base group entered the scene in 2022, but their activity spiked in the middle of 2023[21]. The variant utilised by 8base scans the network, disables Windows firewall, system recovery, backup and shadow copies, and only deploys partial encryption for files over 1.5 MB to improve the process speed[22]. Based on the maturity and activity of the developers of Phobos ransomware and the 8base group, both remain an active threat.

DOPPELPAYMER RANSOMWARE MEMBERS ARRESTED

On 28 February 2023, the German Regional Police, the Ukrainian National Police, the Dutch Police and the United States Federal Bureau of Investigations, with support from Europol, targeted suspected core members of the criminal network responsible for large-scale cyber-attacks using DoppelPaymer ransomware. This ransomware first appeared in 2019 when cybercriminals started using it to launch attacks against organisations, critical infrastructure and industries. Based on the BitPaymer ransomware and part of the Dridex malware family, DoppelPaymer uses a unique tool capable of compromising defence mechanisms that terminates the security process in the systems it attacks.

Europol Press Release, 6 March 2023, 'Germany and Ukraine hit two high-value ransomware targets'

Other notable ransomware groups of 2023, which do not operate as a service, were Play, Royal, Rhysida and Cl0p. Both Play and Royal emerged in 2022, while Rhysida surfaced in mid-2023. Security researchers have associated all three with operators of now disbanded or inactive ransomware groups[23]. However, of the mentioned groups, Cl0p stood out the most due to their zero-day campaign against the MOVEit file transfer software in May 2023[24], following their previous successful campaign against GoAnywhere MFT a few months earlier[25]. The threat actors behind the ransomware group are experienced, technically advanced and likely to have access to high-end IABs capable of creating zero-day exploits, making it possible for them to carry out sophisticated and time-consuming digital supply-chain attacks.

RAGNARLOCKER RANSOMWARE GROUP TAKEN DOWN

In October 2023, LEAs and judicial authorities from Czechia, France, Germany, Italy, Japan, Latvia, the Netherlands, Spain, Sweden, Ukraine and the United States of America arrested the key member of the RagnarLocker group responsible for numerous high-profile attacks against critical infrastructure around the world. The ransomware's infrastructure was also seized in the Netherlands, Germany and Sweden and the associated data leak website on Tor was taken down in Sweden.

Europol Press Release, 20 October 2023, 'Ragnar Locker ransomware gang taken down by international police swoop'

Aside from the aforementioned supply-chain attacks, ransomware groups/affiliates have mostly been targeting small-and-medium-sized businesses (SMBs). As larger enterprises continue to invest in their cybersecurity (e.g. in-house threat intelligence teams, infrastructure resilience, etc.) a simple cost-benefit analysis guides cybercriminals towards organisations with less secure infrastructures.

Most ransomware operators choose their targets based on the size, likelihood of a pay-out and the effort required to compromise the target's systems. This means that attackers seek out publicly accessible systems and services within the infrastructure (reconnaissance) and assess which of them can be compromised most easily. Gaining initial access can be done through stolen credentials or by exploiting vulnerabilities in the public facing technologies. Ransomware groups and affiliates usually employ IABs, who are essentially penetration testers specialised in certain technologies and applications. Usually the IABs (and their specialisation) that ransomware operators have available to them determine the viable attack surface and therefore influences the target selection process. Some technologies are very common, while others are more sector specific, which is why patterns of some ransomware groups targeting certain sectors might emerge.

Similar to previous years, ransomware operators are continuing to deploy multi-layered extortion tactics. Although attackers still tend to encrypt the compromised systems, the risk of publishing or auctioning the stolen data has become the most relevant pressure point against victims, since many organisations have started to back up their systems on a regular basis.

service growing in popularity is Redline Stealer. (see the chapter on Cryptocurrencies and the dark web: enablers of crime).

QAKBOT BOTNET SHATTERED

In August 2023, an international LE operation shattered the Qakbot malware network, which had been targeting critical infrastructure and businesses across multiple countries, stealing financial data and login credentials. Other cybercriminals had used this malware to commit ransomware attacks, fraud and other cyber-enabled crimes. Active since 2007, this prolific malware (also known as QBot or Pinkslipbot) had evolved over time using various techniques to infect users and compromise systems.

Europol Press Release, 30 June 2023, 'Qakbot botnet infrastructure shattered after international operation'

2.3 Malware-as-a-service

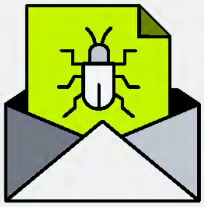
There were several shifts in the malware-as-a-service (MaaS) landscape in 2023. After the takedown of the Qakbot malware infrastructure, cybercriminals reacted quickly and turned to other well-established or up-and-coming dropper/loader service providers. Notable alternatives to QakBot currently used by cybercriminals are IcedID, SystemBC, Pikabot (newly emerged in 2023), DanaBot and Smokeloader (heavily used by 8base group in their campaigns), which offer similar capabilities to obfuscate and deliver malicious payload to infected systems. Another malware

Legitimate penetration testing frameworks* like Cobalt Strike, Metasploit and Mimikatz are widely abused by cybercriminals for establishing persistence and for privilege escalation within compromised systems. Cobalt Strike has been the go-to solution for some time because of its diverse arsenal of capabilities. It is used as a back door** and control-and-command (C2) centre for executing commands, delivering additional payloads and traversing infiltrated networks. The more recent AI-leveraged PentestGPT and similar AI-powered frameworks can also be used with malicious intent to facilitate the initial compromise of information systems.

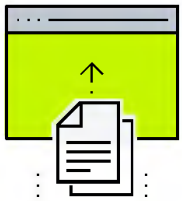
* A penetration testing (pentest) framework is a standardised set of guidelines and suggested tools for structuring and conducting such tests across different networks and security environments. Penetration testing tools are used for adversarial simulation and can emulate the tactics and techniques of attackers in order to test the resilience of networks and environments.

** Cobalt Strike has the ability to create persistent connections between the target and the attackers. Communication can be transmitted over DNS and Windows SMB protocol (in addition to HTTP, HTTPS), which makes the traffic difficult to detect. Beacon can modify its network signature using C2 profiles to make it appear like legitimate network traffic.

HOW DOES QAKBOT WORK?



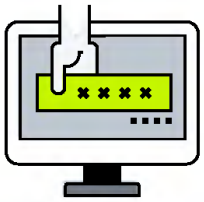
1.The victim receives an email with an attachment or hyperlink and **clicks on it**;



2. Qakbot deceives the victim into **downloading** malicious files by imitating a legitimate process;



3. Qakbot executes and then installs other **malware**, such as banking Trojans;



4. The attacker then **steals** financial data, browser information/hooks, keystrokes, and/or credentials;



5. Other malware, such as **ransomware**, is placed on the victim's computer.

3

Child sexual exploitation

The key threats stemming from online CSE have remained relatively stable throughout 2023. External factors, such as the adoption of new technologies and the increasing unsupervised presence of children online, as well as shifts in the focus of investigative work, have contributed to the evolution of the threats posed by this crime area. CSE continues to be one of the top priorities for LEAs, which are dealing with an ever-growing volume of illegal content online.

Key Developments

- The growing volume of illegal content online is posing greater challenges to the LEAs fighting online child sexual exploitation (CSE). Self-generated sexual material constitutes a significant share of the child sexual abuse material (CSAM) detected online.
- End-to-end encrypted (E2EE) communication platforms are being used more and more by offenders to exchange CSAM and for communication.
- The online sexual extortion of minors is a rising threat, perpetrated by criminals driven by both a sexual interest towards children and financial gain.
- The use of AI, which allows CSE offenders to generate or alter CSAM, is set to further proliferate in the near future. The production of artificial CSAM increments the amount of illicit material in circulation and complicates the identification of victims as well as perpetrators.

3.1 Current CSE threats

Child sexual abuse material (CSAM) keeps proliferating online, continuously victimising the children it depicts and strongly impacting the work of LEAs. With a rising volume of files to manually analyse and the related case information, LEAs find themselves needing innovative technological support to investigate online CSAM. The production and dissemination of CSAM remains a major concern, with a large portion of material detected now identified as self-generated explicit material*.

Live-distant child abuse (LDCA) is a persistent threat, where offenders watch child sexual abuse on demand with the support of one or more facilitators who perpetrate the abuse on the victim(s) in exchange for payment. It stands out as the main form of commercial sexual exploitation of children and as a major source of unknown** CSAM using capping, which entails covertly recording the victim (i.e. in a video call/live-streaming session).

Transnational child sex offenders (TCSOs)*** continue their hands-on abuse of children while travelling to and/or residing in the so-called high-risk countries for victims of CSE****, where they engage with their targets. They operate internationally, sometimes in cooperation with a network of peers and with the support of local facilitators in different locations. Such perpetrators are well connected and produce a significant volume of original CSAM that is further disseminated within offenders' communities online, in which they often play an important role.

* The Luxembourg Guidelines on Semantics and Terminology are currently under revision.

** Unknown CSAM, also called first-generation CSAM, refers to CSAM that authorities are encountering for the first time.

*** This term is currently under revision in the context of the Luxembourg Guidelines on Semantics and Terminology Revision project.

**** Jurisdictions where problematic socio-economic conditions combined with more lenient LE approaches make it easier for perpetrators to seek out victims are generally considered high-risk countries.

Forums and chatrooms are still essential networking environments for CSE offenders who exchange CSAM and discuss abuses perpetrated and fantasies, how to acquire original CSAM, techniques to groom children and OpSec tips. More proficient offenders usually network in dark web forums that appear to be more and more specialised and tailored to sexual preferences. These offenders have increasingly high levels of technical knowledge, and measures to conceal their traces. The forums have specialised sections for technical and OpSec related matters with tips and training options. As these digital environments are often subject to LE takedowns, technical vulnerabilities and Distributed Denial of Service (DDoS) attacks, they usually do not have a lifespan longer than two years. To overcome such issues, the administrators in charge of these forums create mirror sites, holding a copy of its content and, whenever their site is taken down, they quickly recreate it at a new address. End-to-end encrypted (E2EE) communication platforms are increasingly being used by offenders to exchange CSAM and for communication purposes.

3.2 Sexual extortion and violent content online

The volume of self-generated sexual material now constitutes a significant and growing part of the CSAM detected online. This content is created by and depicts children, especially teenagers. In many cases, it is the result of voluntary exchanges among peers but it can be classified as CSAM once disseminated to a third party without the consent of the person who first sent it. Self-generated sexual material is also often the result of online sexual grooming and extortion. In this setting, the perpetrator identifies the victim online, often on gaming platforms or social media, and after gaining their trust through grooming, perpetrators obtain sexually explicit material and use it as leverage for extortion. A feeling of shame and the hope that the threats might stop often lead victims to produce more self-generated sexual material.

In addition to extortion for new CSAM, some offenders also extort money from their victims. Through a similar criminal process, perpetrators approach their victims pretending to be peers looking for a romantic relationship, then turn into blackmailers once they have received the first explicit image from the minor. They threaten the victim that they will share the explicit image online or send it to close contacts. The victim often pays out of shame and, in many cases, the extortion process lasts for a considerable time.

Online groups sharing violent and sexual content, often hosted on E2EE communication platforms, have also been identified as hotbeds for extortion. These groups function as cults where charismatic leaders use deception and manipulation to make their disciples obedient and dependent. Members are pushed to share extreme videos or imagery out of fear, manipulation or behaviour normalisation, while offenders make their demands in search of amusement and sexual gratification. Once the offenders have obtained personal information and sexually explicit material from the victims, they start blackmailing them into producing more sexually explicit and/or extreme self-harm material, often in live sessions for the amusement of other group members. Offenders operating in such groups were often identified as minors who would incite the production and dissemination of all kinds of violent content, including CSAM.

3.3 AI-generated CSAM

AI models able to generate or alter images are being abused by offenders to produce CSAM and for sexual extortion. Such models have developed quickly, with output that now increasingly resembles genuine material, making it harder to identify as artificially generated. AI-generated CSAM has already been reported in 2023 and is expected to become prominent in the near future.

This poses great challenges to LEAs in identifying the real victims as well as the legal framework under which the investigation should fall. Even in the cases when the content is fully artificial and there is no real victim depicted, AI-generated CSAM still contributes to the objectification and sexualisation of children. The generation of these types of artificial images increases the amount of CSAM material in circulation and makes it harder to identify both victims and perpetrators. This production process is also widely available and does not require high levels of technical expertise, potentially broadening the number and spectrum of perpetrators. These files can easily be



used for cyberbullying* or for sexual extortion.

The greater the volume of artificial CSAM in circulation, the more difficult it will become to identify offenders or victims through image recognition. In order to counter such emerging challenges, specialised CSE investigators will have to find new investigative pathways and tools.

CYBERBULLYING WITH AI-ALTERED CSAM

LEAs in Spain looked into its first cases of image manipulation with AI linked to cyberbullying in 2023. The suspects, all minors and some younger than 14 years old, were taking pictures of at least 22 young girls and digitally altering those images with an AI powered application in order to convert them into sexually explicit images and perpetrate acts of cyberbullying. The artificial images were then widely disseminated on social media and communication applications, with the victims suffering significant psychological damage.

Reuters, 25 September 2023, 'Spanish prosecutor to probe AI-generated images of naked minors'

* Cyberbullying is bullying with the use of digital technologies. It can take place on social media, messaging platforms, gaming platforms or mobile phones. It is repeated behaviour that aims to frighten, rile or shame its victims.

4

Online and payment fraud schemes

Online and payment fraud schemes represent a growing crime threat in the EU and beyond, resulting in millions of EU citizens targeted and billions of euros stolen. Investment fraud and business email compromise (BEC) remain the most prolific online fraud schemes. The availability of phishing-as-a-service is growing, with digital skimming posing another major threat, especially to e-merchants.

Key Developments

- Phishing persists as the most prevalent attack vector for fraud and in terms of the number of phishing campaigns against EU citizens, private companies, and public institutions. Smishing (SMS/text phishing) was the most common type of phishing used by fraudsters in 2023, while quishing (QR code phishing) is an emerging threat.
- The availability of phishing-as-a-service is ever increasing. Phishing kits are widely available, lowering the level of organisation and technical expertise required to perpetrate fraud.
- AI tools and deepfakes are expanding social engineering opportunities for criminal actors in their deception and manipulation operations.
- Digital skimming is a persistent threat resulting in the theft, sale and misuse of credit card data.

4.1 Phishing

Phishing remained the most commonly used attack vector among online fraud schemes (OFS) in 2023. Smishing (SMS/text phishing) was the most common type of phishing, ahead of the other variants of vishing (voice phishing) and spoofing. Quishing*, or QR code phishing, also emerged in 2023.

Phishing-as-a-service is a fast-growing industry-like market. It provides products, services and victims' data, which enable more and more criminal networks to engage in successful OFS, regardless of their level of organisation and technical expertise. Anyone can request a phishing page for any bank or post office in the EU from phishing-as-a-service providers. There are even several linked cases of bank phishing, with affiliates managing various fake web shops redirecting to fake banking and payment web pages in parallel. Cryptocurrencies are the most common payment method for basic or premium subscriptions to such services.

Besides the most prevalent forms of phishing, a known fraud scheme that surged in 2023 involved thousands of daily 'shock calls' involving spoofing, social engineering and call centres. This mass phenomenon targeted hundreds of thousands of people across the EU. Criminal networks located both in and outside the EU, operating through various local associates, appear to be behind this scheme.

* Quishing is a phishing attack that uses fake QR codes instead of text-based links as in traditional phishing scams. Fraudsters also place fake QR codes in physical locations for victims to scan.

OPERATION ELABORATE – ISPOOF

'iSpoof.cc' was a website that provided criminals with various services including automated Interactive Voice Response (IVR), PIN code intercepts and live call monitoring. The website could be used to target victims worldwide. The successful takedown of this platform in November 2022 led to the initial arrest of 142 suspects, which later increased to 184. The site is estimated to have caused losses in excess of EUR 115 million. The main administrator of the website was sentenced in the UK last year to 13 years and 4 months in prison. He is believed to have received over EUR 2 million in profits from running iSpoof. This sentence marks a significant step forward in the sanctioning of online fraud schemes.

Eurojust Press Release, 22 May 2023, 'Main administrator of iSpoof website sentenced to 13 years'

Europol Press Release, 24 November 2022, 'Action against criminal website that offered 'spoofing' services to fraudsters: 142 arrests'



184
suspects arrested



EUR 115 million
estimated losses

OPERATION COOKIE MONSTER

April 2023 saw the takedown of Genesis Market, one of the most dangerous dark web marketplaces selling stolen account credentials and bots used by hackers worldwide. This international sweep was led by the US FBI and the Dutch Police, supported by Europol, and involved 17 countries. Genesis Market had over 1.5 million bot listings totalling over 2 million digital identities at the time of its takedown. These bots that had infected a victim's device either through malware or account takeover tactics were being used to collect digital fingerprints, cookies, saved logins and autofill data from forms. Genesis Market was accessible from the surface web by invitation only. The ease of access and low prices made it a very popular CaaS resource among hackers.

Europol Press Release, 5 April 2023, 'Takedown of notorious hacker marketplace selling your identity to criminals'



17
countries involved



+ 2 million
digital identities

4.2 Account takeover (ATO)

Recent investigations have shown the growing threat of the illicit trade in personal data as a key form of CaaS. Account takeovers (ATOs) continue to target victims' accounts (online banking, email accounts or social media profiles). Through ATO, criminals are also able to take hold of funds and access victims' digital services or sensitive private information that can then be monetised online. As banks are increasingly treating funds lost through 2FA/MFA credentials scams as negligence on the part of the legitimate account owner, fraud schemes targeting individuals' accounts remain a low-risk and high-profit activity for criminals.

4.3 Investment, BEC and romance fraud

Investment fraud persists as a key threat in the EU[26], targeting thousands of victims and generating millions in illicit profits. Cryptocurrencies continue to be the most reported product offered to victims in investment fraud. Remote Administration Tools (RATs) are an essential for fraudsters running these schemes through victims' devices. There are criminal investment apps available for download on legitimate app stores in different countries and languages. AI-generated advertisements are also being used to lure potential victims and this is set to rise.

BEC and, in particular, CEO fraud, remains a commonly reported type of fraud against EU citizens and private companies[27]. In some cases, fraudsters use phishing techniques to intercept and manipulate corporate communication. Convincing fraud emails can be easily generated with the help of LLMs. Given the growing rise and popularity of generative AI models, unethical LLMs were detected in 2023 and are set to evolve and multiply.

Despite low levels of reporting, mostly due to a sense of shame felt by victims, romance scams remain a major threat[28]. AI tools expand the possibilities for fraudsters not only to reach out to more victims at once, but also to improve their social engineering techniques.

ACTION AGAINST FRAUDULENT ONLINE INVESTMENT PLATFORM: FIVE ARRESTS OF HIGH-VALUE TARGETS

In March 2023, Europol and Eurojust supported German LEAs in coordinated action against a fraudulent online investment platform that has targeted at least 33 000 victims for an estimated loss of EUR 89 million in illicit profits. During the action days, five suspects were arrested and LEAs searched 15 locations in Bulgaria, Romania and Israel, including five illegal call centres. The operation is a follow-up to actions coordinated in 2021 against the same criminal network that had been attracting victims online with promises of high returns for their investments. Investors were encouraged to place money in high-risk financial instruments, such as binary options.

Europol Press Release, 13 April 2023, 'Further action against fraudulent online investment platform: five arrests of high-value targets'

4.4 Digital skimming attacks

Digital skimming remained a key threat in 2023, targeting e-merchant sites. Perpetrators inject malicious code (a.k.a. web skimmers) into an online store website through various methods and techniques.

A digital skimming attack consists of three main parts: loader, malicious attack code and data exfiltration. Web skimmers may be injected directly into the target website's server or by exploiting a vulnerability in an e-commerce platform. Web skimmers could also be placed into a site by exploiting a third-party resource in what is known as a supply-chain attack. In the latter case, if a page contains code from another domain, an attacker can inject malicious code and bypass most of the security measures. The data exfiltration is the method used to transmit the stolen data to the attacker's C2 server.

4.5 ATM attacks

Fraud attacks at terminals in the EU decreased by 40 % in the first half of 2023 compared to 2022[29]. This decrease was primarily due to a fall in cash trapping performed by fraudsters at ATMs (placing a cover in front of the slot so that the money cannot come out of the machine). Man-in-the-middle and relay attacks continue to occur, resulting in cash-out attacks at ATMs[30].

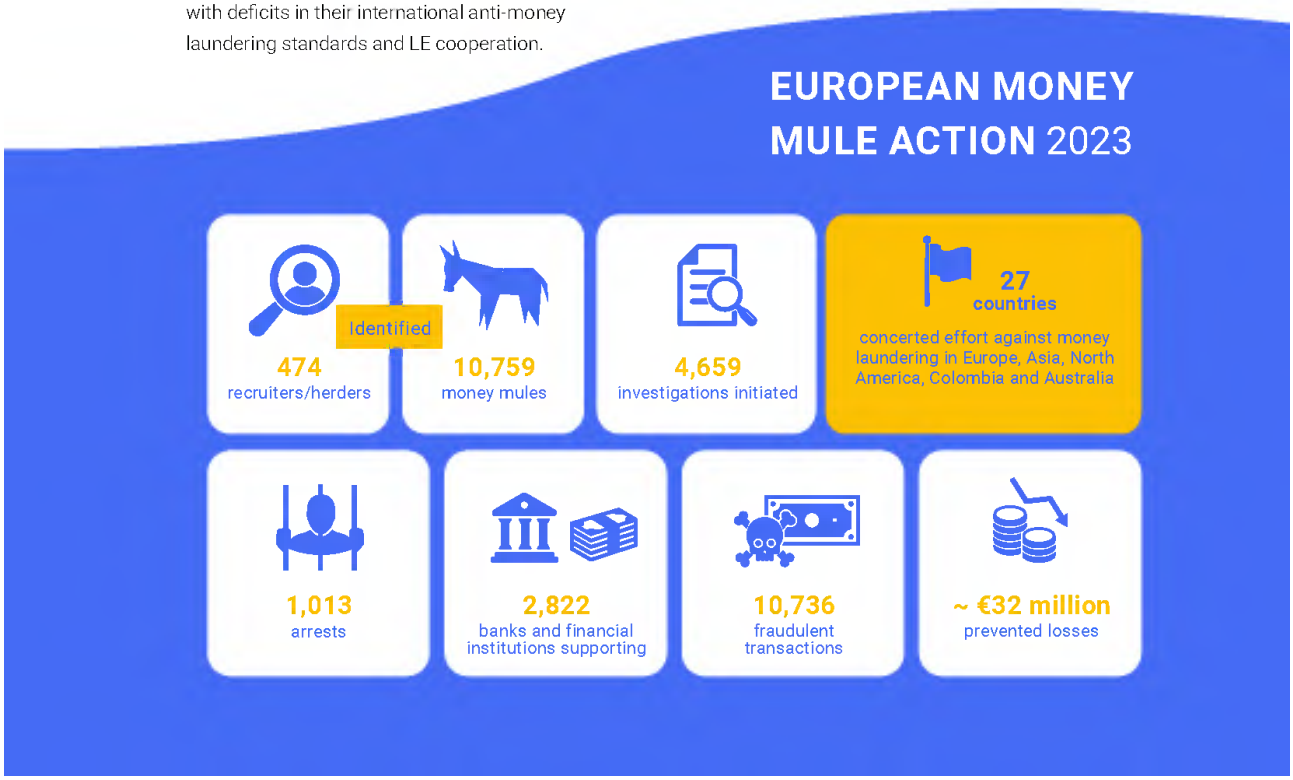
4.6 Online fraud and money laundering

Fraud, especially investment-related fraud, is the most frequently identified predicate offence involving the illegal use of cryptocurrencies[31]. As fraudsters are levelling up their obfuscation techniques for money laundering, they increasingly rely on digital banking solutions, underground banking and criminal finances, and on non-compliant crypto service providers with insufficient levels of KYC. Moreover, the misuse of virtual IBANs (vIBANs) remains a potentially growing threat[32]. However, money muling and other more traditional money laundering methods have also cropped up in recent investigations with some steps of the criminal process spread across jurisdictions with deficits in their international anti-money laundering standards and LE cooperation.

EUROPEAN MONEY MULE ACTION (EMMA) 9

In June, October and November 2023, a total of 26 countries, supported by Europol, Eurojust, INTERPOL and the European Banking Federation (EBF), hit money mules and their recruiters in a series of coordinated operations. The annual iteration of operation EMMA identified 10 759 money mules, with 474 recruiters and 1 013 individuals arrested worldwide. 2 822 banks and financial institutions collaborated with LE, as did online money transfer services, cryptocurrency exchanges, online travel providers and KYC companies, and multinational computer technology corporations.

Europol Press Release, 4 December 2023, 'Paper trail ends in jail time for 1 013 money mules'



5

Outlook: what to expect in the near future



5.1 AI-assisted cybercrime has only just begun

The wider adoption of AI tools and services by cybercriminals creates novel threats, involving both the abuse of legitimate tools and services and their malicious versions created ad-hoc by offenders. The growing number of LLMs without prompt filtering which emerged recently is set to multiply and there will likely be more and more AI-generated advertisements luring in potential victims to online fraud. AI being used to improve criminal methods and scripts (e.g. to hack digital exchanges and liquidity protocols in order to steal funds) is another possible scenario. Abuse of LLMs might allow criminals to overcome language barriers so that sex offenders are able to groom victims virtually in any language, impersonating peers and interacting in a way that the victim perceives as natural and believable. Malicious LLMs will become even more prominent within the umbrella of crime-as-a-service (CaaS).

AI-assisted CSAM is another worrisome threat that will need close monitoring. Instances of AI-altered and fully artificial CSAM will pose growing challenges to LE investigations, not only in terms of the volume of CSAM in circulation but also to the ability of investigators to identify the true identity of victims and offenders. AI tools will lower the entry barrier to cybercrime, meaning that individuals with limited technical expertise will be able to carry out cyber-attacks and orchestrate quite sophisticated online fraud schemes.

Cybercriminals involved in CSE and online fraud will continue to take advantage of deepfake technology as its quality improves and it becomes easier to access. Such technology could be further abused in sexual extortion cases, as offenders produce fake content to threaten victims. This trend would require LEAs to have more suitable and sophisticated tools to identify which (parts of) audio, image and video content are deepfakes[33].

5.2 Abusing technologies

Mainstream E2EE communication platforms are increasingly used by offenders. The current regulatory framework regarding the protection of personal communications via E2EE creates challenges for LEAs lawful access* to criminal communications.

* Lawful access to data refers to the legal procedures and mechanisms that allow authorised government or law enforcement agencies to access, obtain, or request information from service providers. This access is typically regulated by laws and policies to ensure that privacy rights are protected and that the process follows legal protocols.

Wider adaptation of Web3 principles will lead to a further decentralised Internet. In a decentralised Internet, communications are neither controlled nor regulated by governments or private companies[34]. Blockchain technology and P2P networks are two types of decentralised communication networks consisting of privately owned platforms controlled entirely by the users[35]. Decentralisation, blockchain technology and P2P networks will continue to provide opportunities for cyber offenders as they make it easier to carry out transactions anonymously and out of sight of the authorities.

5.3 Emergence of new RaaS brands

It is likely that new RaaS brands will emerge, but their longevity will largely depend on the experience and sophistication of the criminal actors behind the operations. Since many ransomware groups operate in countries with limited judicial cooperation, the LEAs approach of disrupting and taking down criminal services to sow distrust towards their brands will be the way forward.

5.4 Protecting EU payment systems

Ongoing reforms of the regulatory mechanisms for payment services will hopefully have a positive impact on online and payment fraud. In June 2023, the European Commission unveiled a series of proposals – including for the Payment Services Directive 3 ('PSD3') and the Payment Services Regulation ('PSR') – to better combat and mitigate payment fraud. PSD3 encourages Payment Institutions (PIs) to voluntarily share information related to fraud for better inter-institutional collaboration. In addition to enhanced information sharing, PSD3 extends refund rights for consumers who fall victims to spoofing scams, where fraudsters impersonate PI employees.

The current version of the Payment Card Industry Data Security Standard (PCI DSS)* has been retired on 31 March 2024, with the new version coming into force in June 2025. The new standards are aimed at boosting capacity in preventing major skimming attacks. For instance, businesses accepting credit card payments will have to be aware of what scripts are running on their online payment pages, how those scripts behave, and when those scripts change. In addition, e-merchants that include a third-party service providers (TPSP's) inline frame (iframe) payment form must be able to evaluate the HTTP headers as well as detect unauthorised script changes on the payment page itself, and to raise alerts on any script changes.

5.5 Bolstering the EU against illicit content online

A key EU instrument to counter online threats is the EU Digital Service Act, which entered into force on 17 February 2024[36]. This EU Regulation aims to provide a safer experience for everyone within the online ecosystem by prompting digital services operating in the EU to improve transparency and accountability. The DSA targets online platforms, search engines, hosting services and intermediary services offering network infrastructure, and it sets out a number of ways to counter illegal content, goods and services. These include the obligation for online marketplaces to improve their KYC practices, the introduction of a system of trusted flaggers for counterfeit and unsafe goods, bans on advertising targeting minors or based on ethnicity, political views or sexual orientation. The DSA also sets out obligatory mitigation measures for large online platforms against risks such as disinformation, or election manipulation, cyber violence against women, or online harm against children.

5.6 The future of crypto

Several developments in the cryptocurrency market are set to have a significant impact on criminals' abuse of cryptocurrencies in many forms of cybercrime in the near future. January 2023 saw the

* The Payment Card Industry Data Security Standard (PCI DSS) is a global set of security standards defined by the Payment Card Data Security Council to protect payment card data against evolving cybersecurity threats. Any organisation that processes payment cards online, from small start-ups to large global enterprises, must adhere to every requirement outlined in the PCI DSS to remain compliant.



launch of Bitcoin ordinals* allowing users to create non-fungible tokens (NFTs) on the Bitcoin blockchain. For now, it is technically difficult to create ordinals and it will likely not be adopted en masse, however it remains potentially exploitable by cybercriminals.

Other criminal trends around the Bitcoin exchange-traded funds (ETFs) may also emerge. The first Bitcoin ETF was approved in January 2024, to allow investors to speculate on Bitcoin's price without directly owning Bitcoins[37]. This development may lead to an increased mainstream adoption of Bitcoin**. However, scammers could abuse the rise of ETFs related to cryptocurrencies as people who do not have extensive experience in cryptocurrency will become increasingly exposed to them. Companies issuing cryptocurrency ETFs will also have to hold large reserves in cryptocurrency, which might make them valuable targets for fraudsters.

5.7 Renewed focus on offender prevention

By prioritising offender prevention, LEAs and policymakers can address cybercrime at its core, leading to more sustainable and long-term solutions in safeguarding cyberspace. By targeting the root causes that drive individuals towards engaging in cybercriminal activities, such as lack of awareness, financial incentives or socio-economic factors, authorities can effectively reduce online crime rates.

Investing in offender prevention not only mitigates against the immediate risks posed by cyber threats but also helps cultivate a culture of cybersecurity, fostering a safer digital environment for individuals, businesses and governments alike.

When looking at cybercrime offender profiles, the majority of criminals are young, especially considering the disruptive nature of this crime area and its harm potential. While their offences damage their victims, they also have a potentially far-reaching impact on their own future, as many of these individuals are unaware of the legal consequences of what they view as a mere challenge or a game. Cybercriminals typically do not face consequences until they are further down their criminal path, often encountering law enforcement for the first time through an arrest. Their advanced digital skills could be instead redirected towards legal avenues that contribute positively to society. In the EU, Cyber Offender Prevention (COP) is gaining recognition as a crucial strategy, alongside investigative measures, to effectively combat cybercrime.

In this framework, since 2023 Europol has been supporting the InterCOP network[38]. The network composed of international LEAs that share expertise and jointly develop, implement and evaluate COP interventions and prevention campaigns. The network engages with public and private sector stakeholders whose skills, resources and reach are needed, alongside LE efforts, to create a safer digital environment.

* Ordinals allow for the creation of non-fungible tokens (NFTs) on the Bitcoin blockchain. Images, videos or other content can now be inscribed directly onto the blockchain. Previously, only transactional data could be stored there.

** At the end of February 2024, the price of Bitcoin had surged to its highest levels since the last bull market in 2021.

References

1 Europol Press Release, 21 April 2024, European Police Chiefs call for industry and governments to take action against end-to-end encryption roll-out, accessible at https://www.europol.europa.eu/media-press/newsroom/news/european-police-chiefs-call-for-industry-and-governments-to-take-action-against-end-to-end-encryption-roll-out

2 Council of the EU Press Release, 16 May 2023, 'Anti-money laundering: Council adopts rules which will make crypto-asset transfers traceable', accessible at https://www.consilium.europa.eu/en/press/press-releases/2023/05/16/anti-money-laundering-council-adopts-rules-which-will-make-crypto-asset-transfers-traceable/

3 European Banking Authority Press Release, 16 January 2024, 'EBA issues guidance to crypto-asset service providers to effectively manage their exposure to ML/TF risks', accessible at https://www.eba.europa.eu/publications-and-media/press-releases/eba-issues-guidance-crypto-asset-service-providers

4 Munitio Dark Web Monitoring, 23 February 2023, 'A deep dive into the Russian Cybercrime Forums shaping 2023's landscape', accessible at https://munit.io/a-deep-dive-into-the-russian-cybercrime-forums-shaping-2023s-landscape/, Flare, 6 June 2023, Exploit Forum, 'Initial Access Brokers, and Cybercrime on the Dark Web', accessible at https://flare.io/learn/resources/blog/exploit-forum/, Socradar, 12 July 2022, 'Top 5 Dark Web forums', accessible at https://socradar.io/top-5-dark-web-forums/

5 United States Department of Justice, Office of Public Affairs Press Release, 24 March 2023, 'Justice Department Announces Arrest of the Founder of One of the World's Largest Hacker Forums and Disruption of Forum's Operation', accessible at https://www.justice.gov/opa/pr/justice-department-announces-arrest-founder-one-world-s-largest-hacker-forums-and-disruption

6 Cybernews, 22 June 2023, 'BreachForums is back – for real this time', accessible at https://cybernews.com/security/breachforums-back-online/

7 ComputerWeekly, 15 May 2024,' US authorities crack BreachForums for a second time', accessible at: https://www.computerweekly.com/news/366585206/US-authorities-crack-BreachForums-for-a-second-time

8 Webz, Dark Web News, 19 June 2023, 'All about RAMP Ransomware Forum', accessible at https://webz.io/dwp/all-about-ramp-ransomware-forum/

9 Webz, Dark Web News, 15 November 2023, 'The Top 10 Dark Web Marketplaces in 2023', accessible at https://webz.io/dwp/the-top-10-dark-web-marketplaces-in-2023/

10 404media, 5 February 2024, Features, 'Inside the Underground Site Where 'Neural Networks' Churn Out Fake IDs', accessible at https://www.404media.co/inside-the-underground-site-where-ai-neural-networks-churns-out-fake-ids-onlyfake/

11 Security Week, 2 March 2022, 'Conti Ransomware Source Code Leaked', accessible at https://www.securityweek.com/conti-ransomware-source-code-leaked/

12 The Hacker News, 26 August 2023, 'LockBit 3.0 Ransomware Builder Leak Gives Rise to Hundreds of New Variants', accessible at https://thehackernews.com/2023/08/lockbit-30-ransomware-builder-leak.html

13 Bleeping Computer, 9 October 2023, 'HelloKitty ransomware source code leaked on hacking forum', accessible at https://www.bleepingcomputer.com/news/security/hellokitty-ransomware-source-code-leaked-on-hacking-forum/

14 US Justice Department, Press Release, 19 December 2023, Justice Department Disrupts Prolific ALPHV/Blackcat Ransomware Variant', accessible at https://www.justice.gov/opa/pr/justice-department-disrupts-prolific-alphvblackcat-ransomware-variant

15 Bleeping Computer, 5 March 2023, Blackcat ransomware shuts down in exit scam, blames the ''feds'', accessible at https://www.bleepingcomputer.com/news/security/blackcat-ransomware-shuts-down-in-exit-scam-blames-the-feds/

16 More information is available https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

17 TrendMicro, 25 July 2022, 'LockBit Ransomware Group Augments Its Latest Variant, LockBit 3.0, With BlackMatter Capabilities', accessible at https://www.trendmicro.com/en_us/research/22/g/lockbit-ransomware-group-augments-its-latest-variant--lockbit-3-.html

18 ObjectiveSee, 16 April 2023, 'The LockBit ransomware (kinda) comes for macOS', accessible at https://objective-see.org/blog/blog_0x75.html

19 TrendMicro Research, 5 October 2023, Ransomware Spotlight, Akira, accessible at https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-akira

20 Talos Intelligence (Cisco), 17 November 2023, 'Understanding the Phobos affiliate structure and activity', accessible at https://blog.talosintelligence.com/understanding-the-phobos-affiliate-structure/

21 VmWare Security Blog, 28 June 2023, '8Base Ransomware: A Heavy Hitting Player', accessible at https://blogs.vmware.com/security/2023/06/8base-ransomware-a-heavy-hitting-player.html

22 Talos Intelligence (Cisco), 17 November 2023, 'A deep dive into Phobos ransomware, recently deployed by 8Base group', accessible at https://blog.talosintelligence.com/deep-dive-into-phobos-ransomware/

23 Unit 42, 9 May 2023, 'Threat Assessment : Royal Ransomware', accessible at https://unit42.paloaltonetworks.com/royal-ransomware/ , TrendMicro, 21 July 2023, 'Ransomware Spotlight, Play', accessible at https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-play , Check Point Research, 8 August 2023, 'The Rashyda Ransomware, Activity Analysis and Ties to Vice Society', accessible at https://research.checkpoint.com/2023/the-rhysida-ransomware-activity-analysis-and-ties-to-vice-society/

24 CyberInt, 15 August 2023, 'MOVEit Supply Chain Attack Campaign August Update' ,accessible at https://cyberint.com/blog/research/moveit-supply-chain-attack/

25 Cybersecurity and Infrastructure Security Agency, Cybersecurity Advisory, 7 June 2023, '#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability', accessible at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a

26 Europol, 27 September 2023, 'The other side of the coin – An Analysis of Economic and Financial Crime – European Financial and Economic Crime Threat Assessment 2023', accessible at https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime

27 Ibid.

28 Ibid.

29 European Association for Secure Transactions (EAST), 17 October 2023, 'Terminal related fraud attacks fall in Europe', accessible at https://www.association-secure-transactions.eu/terminal-related-fraud-attacks-fall-in-europe/

30 Ibid.

31 Ibid.

32 Europol, 27 September 2023, 'The other side of the coin – An Analysis of Economic and Financial Crime – European Financial and Economic Crime Threat Assessment 2023', accessible at https://www.europol.europa.eu/publications-events/publications/other-side-of-coin-analysis-of-financial-and-economic-crime

33 INHOPE, 14 July 2021, 'What is a Deepfake?', accessible at https://inhope.org/EN/articles/what-is-a-deepfake

34 Hackl, C., Lueth, D. & Di Bartolo, T., 2022, Navigating the Metaverse: A Guide to Limitless Possibilities in a Web 3.0 World, published by Wiley.

35 Blockchain Council, 1 September 2022, 'Blockchain & Role Of P2P Network', accessible athttps://www.blockchain-council.org/blockchain/blockchain-role-of-p2p-network/ Yaga, D., Mell, P., Roby, N., & Scarfone, K., 2019, Blockchain technology overview, accessible at https://nvlpubs.nist.gov/nistpubs/ir/2018/nist.ir.8202.pdf

36 More information on the Digital Service Act is available at https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348

37 Reuters, 11 January 2024, 'US SEC approves bitcoin ETFs in watershed for crypto market', accessible at https://www.reuters.com/technology/bitcoin-etf-hopefuls-still-expect-sec-approval-despite-social-media-hack-2024-01-10/

38 More information on the InterCOP initiative can be found at https://www.europol.europa.eu/partners-collaboration/networks/intercop-international-cyber-offender-prevention-network ; https://www.politie.nl/en/information/what-does-the-the-international-cyber-offender-prevention-network-intercop-do.html


EUROPOL
This publication and more information on Europol are available on the Internet.
www.europol.europa.eu