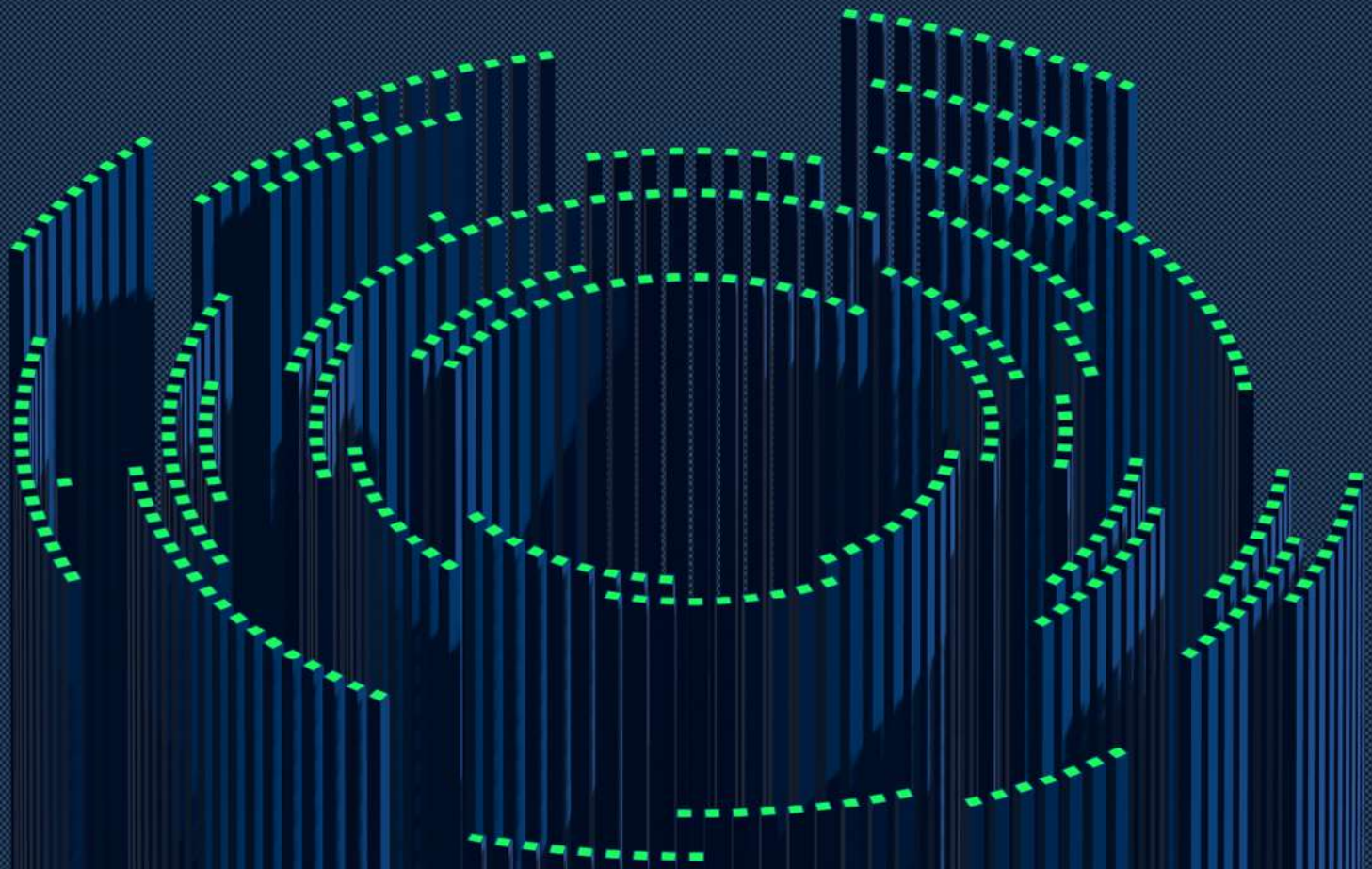
EUROPOL



IOCTA 2026

Internet Organised Crime Threat Assessment

The evolving threat landscape

How encryption, proxies and AI are expanding cybercrime

The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime.
Internet Organised Crime Threat Assessment (IOCTA) 2026

PDF WEB

ISBN 978-92-9414-096-8 ISSN 2363-1627 doi: 10.2813/5737847 QL-01-26-004-EN-N

Luxembourg: Publications Office of the European Union, 2026

Cite this publication: Europol, *The evolving threat landscape. How encryption, proxies and AI are expanding cybercrime – Internet Organised Crime Threat Assessment (IOCTA) 2026*, Publications Office of the European Union, Luxembourg, 2026.

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

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

I am pleased to present Europol's Internet Organised Crime Threat Assessment (IOCTA) 2026, the most comprehensive analysis of the latest threats and trends in cybercrime in the EU. This report also serves as a critical call to action for all stakeholders committed to safeguarding our society in the digital domain and beyond.

The accelerating pace of cybercrime presents progressively sophisticated threats to society, with harmful implications both online and offline. As we release this year's report "How encryption, proxies, and AI are expanding cybercrime", it is clear that law enforcement must step up to address these evolving challenges.

Cybercriminals are rapidly exploiting advanced technologies, particularly AI tools, to enhance the speed, efficiency, and scope of their illicit activities. These tools not only enable automation in criminal processes but also blur the lines between legitimate and malicious uses of technology.

The widespread use of end-to-end encryption platforms and complex jurisdictional barriers create significant investigative challenges, hindering the identification of suspects and the corroboration of evidence. Moreover, restrictive data retention policies often leave law enforcement authorities unable to access crucial data in a timely manner, impeding their ability to track suspects and disrupt criminal operations.

The resilience and adaptability of dark web marketplaces and forums, coupled with the use of cryptocurrencies, further complicate the efforts of policing in the digital domain. The current online fraud epidemic, the threat posed by ransomware intertwining with hybrid threats, and the monetisation of child sexual abuse material underscore the urgent need for more proactive and collaborative efforts.

This call to action resonates deeply, and I am committed to ensuring that Europol leads the way in this critical endeavour. Together, we can build a more secure and resilient digital.

Catherine De Bolle
EXECUTIVE DIRECTOR OF EUROPOL

Introduction

The accelerating pace of cybercrime presents increasingly sophisticated threats for society – with harmful implications both online and offline. In parallel, it introduces additional challenges for law enforcement, which must overcome the widening 'velocity gap'. As AI tools become more accessible, cybercriminals are able to lower the barrier to entry, scale operations more effectively, and increasingly commit crimes without direct involvement in the operations. This evolution means that criminals will likely minimise the time needed to launch attacks, while increasing both their scale and personalisation. Law enforcement authorities (LEAs), therefore, must adopt and integrate AI capabilities proactively to anticipate, understand, and mitigate emerging threats, ensuring society's security in the digital domain while respecting fundamental rights and data protection.

The challenges of investigating and prosecuting cybercrime: Data and jurisdictional barriers

The widespread criminal use of end-to-end encryption (E2EE) platforms, coupled with complex jurisdictional and technical barriers, creates significant investigative blind spots. These obstacles hinder the identification of suspects and the corroboration of evidence, ultimately slowing down investigations and weakening preventive actions against imminent threats. To close this gap and counter the abuse of E2EE applications, LEAs must advocate for regulatory frameworks and expand collaborative initiatives with online service providers (OSPs).

Moreover, LEAs are often hampered by restrictive or inadequate data retention policies. By the time investigators request access to relevant data, it is often no longer available, impairing their ability to track suspects or disrupt criminal operations. The alignment of data retention policies across digital service providers, not just in terms of retention duration but also regarding which data is kept, would significantly enhance LE capabilities.

Cybercrime enablers: Resilient, adaptable, and sophisticated

The resilience of dark web marketplaces and forums plays a critical role in facilitating cybercrime. These platforms are becoming increasingly specialised and fragmented, intertwining more and more with E2EE messaging platforms, in a hybrid ecosystem of anonymity. Despite continuous takedowns by LEAs, these criminal actors show remarkable adaptability, with new platforms emerging rapidly to replace those that are disrupted.

Cryptocurrencies remain the preferred payment method for cybercriminals, particularly in ransomware attacks. The growing use of high-opacity coins and mixing services further complicates LEAs' ability to track illicit financial flows. With the increasing overlap between surface and dark web channels, enabled by E2EE and anonymised services, cybercriminals are conducting near-real-time crypto transactions. This enhances their ability to launder money across both the cybercrime and wider organised crime landscape.

Cybercriminals continue to exploit both commercial

E2EE platforms and decentralised protocols. As these technologies become more accessible, they allow criminals to operate with a larger user base, further complicating LE efforts. The strategic use of bullet-proof hosting, infrastructure spread across multiple jurisdictions, and layered routing schemes via residential proxies make it increasingly difficult for LEAs to detect and track criminal activity.

Online fraud schemes: A growing threat

Fraud schemes represent the fastest-growing area of organised crime. Criminal networks target both individuals and organisations, generating substantial profits from schemes like investment fraud, business email compromise (BEC), and fraud against online payment systems. Investment fraud, particularly related to cryptocurrencies, is especially prevalent.

Online fraud schemes (OFS) networks operate as highly efficient, transnational industries, utilising a range of logistical, technical, and financial operations to perpetrate large-scale fraud. Phishing, the use of SIM boxes, and malicious advertising are common tactics used to steal funds and personal information. With the increasing adoption of generative AI, fraudsters can now personalise social engineering techniques, making them more convincing and dangerous.

The use of crime-as-a-service (CaaS), where fraudsters can outsource criminal activities like cryptocurrency theft, further expands the reach of online fraud. As AI tools become more sophisticated but also mainstream, the threat posed by OFS is set to further escalate, with automated processes enhancing the speed and scale of victimisation.

Ransomware: A complex and evolving landscape

Ransomware remains a dominant threat across the EU, with more than 120 active ransomware brands observed by Europol in 2025. Criminal actors continue to exploit vulnerabilities in the digital supply chain and employ increasingly sophisticated social engineering techniques. The extortion model continues shifting from encrypting data to pressuring victims to pay for their data to not be released.

While financial gain remains the primary driver of cyber-attacks, the relationship between hybrid threat actors and cybercriminals is blurring. Hybrid threat actors are increasingly using cybercriminal networks as proxies for disruptive operations, including DDoS attacks, intrusions, and ransomware attacks. In the growing CaaS economy, hybrid threat actors are simply another customer, further complicating efforts to counter these multifaceted threats.

The ransomware landscape continues to evolve with the expansion of ransomware-as-a-service (RaaS), as criminal actors adapt their platforms and launch new services to attract affiliates. There is also a continuous proliferation of extortion tactics that criminals use to apply psychological pressure on victims, including data exfiltration, DDoS attacks, and cold-calling.

Child sexual abuse material (CSAM): New technologies and monetisation

Child sexual exploitation (CSE) offenders are rapidly adapting to new technologies, expanding their crimes, upscaling abuse opportunities, and making the exchange of CSAM more efficient, while simultaneously complicating law enforcement efforts. The trade in CSAM is growing, with offenders exploiting online platforms for both the production and distribution of illicit material. Live distant child abuse (LDCA) in particular, remains a persistent challenge as the lack of evidence in these crimes makes them difficult to investigate.

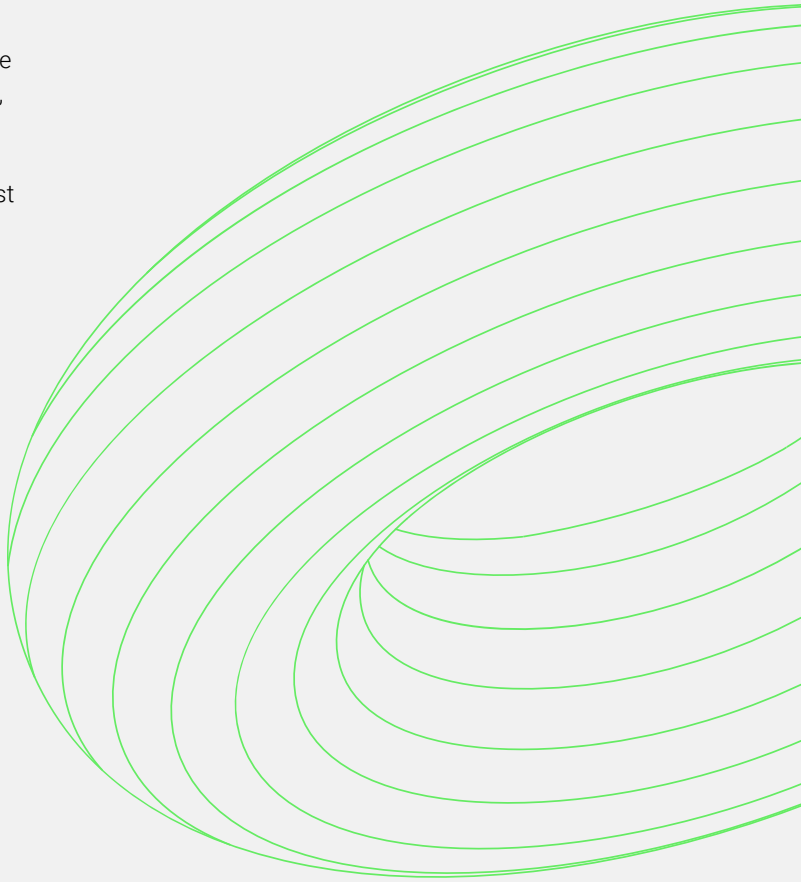
The trade in CSAM for financial gain is increasing, and multi-layered extortion models are also becoming more common, with offenders manipulating victims to produce more content, send money or commit violent acts. The rise of AI-generated CSAM poses additional challenges for victim identification and investigative capabilities. As the trade grows, more platforms selling CSAM also emerge.

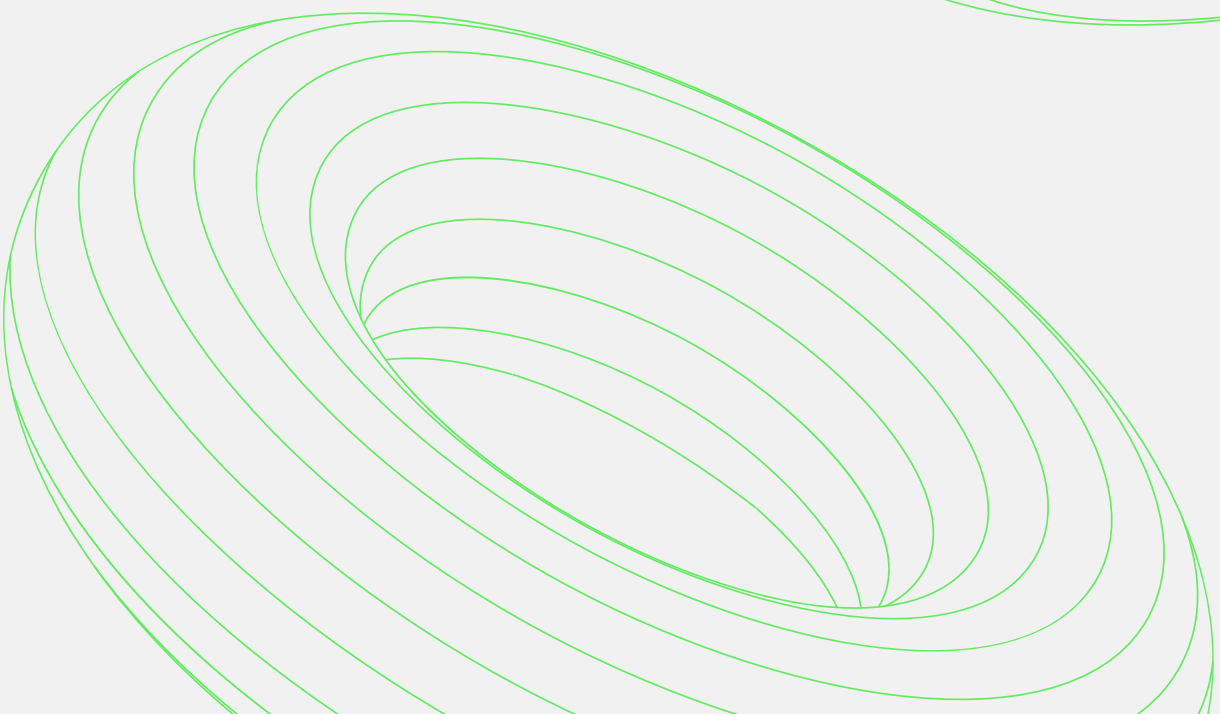
The exploitation of E2EE platforms by CSE offenders and online extortion communities such as The Com network pose extremely serious threats to children and to society, creating a complex criminal landscape where CSE, cyber-attacks, extortion, assault, rape, murder, and violent extremism intertwine.

Looking ahead

The landscape of cybercrime will continue to rapidly evolve, driven by increasingly sophisticated tools and methods. To effectively combat these threats, LEAs must invest in AI capabilities, improve cross-border cooperation, and advocate for stronger data retention and lawful access policies. As criminals exploit new technologies and create complex networks, law enforcement must adapt quickly to ensure the safety and security of the digital world.

In the coming years, law enforcement's ability to tackle cybercrime will depend on its capacity to bridge this 'velocity gap' by harnessing technology. However, the rapid evolution of cybercrime will require more than just technological integration - it will require closer collaboration with the private sector. LEAs must secure access to the vast data held by online service providers (OSPs), in order to identify and apprehend criminals and terrorists effectively.





CYBERCRIME ENABLERS

01

Key Developments

- Dark web marketplaces are increasingly fragmented, moving towards more specialised platforms catering to specific criminal activities. Despite ongoing takedowns and law enforcement efforts, marketplaces demonstrate remarkable resilience, with new ones emerging rapidly to replace those disrupted. Forums function as migration hubs after a prominent market is closed down.
- Cryptocurrencies continue to serve as the preferred payment method for ransomware attacks. A growing trend towards high-opacity coins resistant to blockchain tracing tools poses new challenges to law enforcement authorities. Mixing services frequently located in offshore jurisdictions are making the tracking of illicit transactions even more challenging.
- The distinction between surface and dark web communication channels is becoming increasingly blurred, as E2EE platforms and anonymised services now connect the two realms.
- The abuse of the Domain Name System (DNS) allows criminals to effectively exploit the time period between domain registration and LE intervention.
- Criminals are moving towards more complex operational set-ups, hosted on sub-sub-leased servers or self-deployed infrastructure, routed through multiple obfuscation layers and increasingly masked by residential proxies, which makes them significantly harder for LEAs to trace and dismantle.

In the fast-evolving cybercrime landscape, various enablers facilitate illicit operations, creating a complex environment that challenges LE investigations. The fragmented yet resilient nature of dark web marketplaces and forums serves as primary entry point for cybercriminals. Cybercriminal are implementing more layers in their infrastructures to further challenge their tracing and identification.

Among the facilitators of financial cybercrime, privacy coins and off-shore exchange services play a pivotal role in the laundering of ransomware payments. Besides, the integration of automation and AI in cybercrime operations pose several future threats. Criminal networks also continue to abuse the DNS for both cyber-attacks and online fraud schemes (OFS), where slow reporting mechanisms undermine mitigation and prevention efforts.

1.1 The dark web ecosystem

In 2025, the dark web continued to function as a critical enabler within the global cybercrime ecosystem, providing operational infrastructure, services, and anonymity. While LEAs are able to exert pressure through takedowns, dark web forums continue to shape the underground economy. The dark web continued to demonstrate resilience and dynamism, as marketplaces adapt, user migration becomes easier and faster, and communication platforms diversify.

Marketplaces: fragmentation, specialisation and resilience

General-purpose marketplaces, once the dark web core hubs for illicit trade, have shown signs of contraction. The average lifespan of criminal markets further shortened and administrators appear increasingly risk-averse due to international LEA actions. Following takedowns, users migrate to other marketplaces, moving where the number of listings rapidly increases. Markets do not have enough time to build up large user numbers anymore, leading to a fragmentation, internal instability and widespread mistrust among users.

Smaller, dedicated platforms continued to gain traction[1]. They focus on mediating tools and services for fraud (bank accounts, one-time password (OTP) bypass tools, compromised card data), access brokerage (compromised RDP/VPN credentials), malware services (stealers, droppers, loaders), etc. Smaller communities improve the operational security of the platform by limiting exposure and enable administrators to vet or restrict memberships.

However, dedicated marketplaces also experience instability, with exit scams via sudden shutdowns remaining endemic. Administrators increasingly plan shutdowns, to disappear with users' funds at the first sign of trouble. Shutdown plans involve coordinated deletion, rapid infrastructure turnover, and exit scams. These safeguards reduce the window for asset seizure and hamper digital forensic analysis of seized devices.

EUROPE-WIDE TAKEDOWN HITS LONGEST-STANDING DARK WEB DRUG MARKET

Archetyp Market operated as a drug marketplace since 2020, amassing more than 600 000 users worldwide, with a total transaction volume of at least EUR 250 million. With over 17 000 listings, it was one of the few dark web markets that allowed the sale of fentanyl and other highly potent synthetic opioids, contributing to the growing threat posed by these substances in the EU and beyond. In June 2025, a large-scale LE operation, supported by Europol and Eurojust, led to the dismantlement of the market. Coordinated actions took place across Germany, the Netherlands, Romania, Spain, and Sweden, targeting the platform's administrator, moderators, key vendors, and technical infrastructure. The platform's infrastructure was based in the Netherlands, while its administrator – a 30-year-old German national – was arrested in Barcelona, Spain. Measures were taken in Germany and Sweden against one moderator and six of the marketplace's highest vendors, and assets, worth EUR 7.8 million, were seized[2].

Shortly after the takedown of Archetyp Market, **Abacus Market** (once the largest market in listings) and **MGM Grand** (with more than 15 500 listings) shut down. As the largest remaining Bitcoin-enabled markets, their wide userbase made them vulnerable to heightened LE scrutiny and potential intervention. LE actions potentially prompted administrators to choose self-preservation and exit scamming over risks of seizure.

A new marketplace called **BlackOps** was then launched in July 2025. It immediately listed 41 942 items, and then grew to 63 979 by the end of November 2025. This growth underscores the hypothesis that the shutdown of popular markets triggers user migration and identification of new opportunities for criminal action. Together with **TorZon** and **Nexus Market**, the three quickly became the marketplaces with the largest number of listings by the end of the year.

Forums as the primary entry vector

Forums remain key entry points for aspiring cybercriminals and provide a critical environment to advertise leaked or breached data listed on marketplaces. They also provide onboarding, tutorials, and MO development, trust-based social structures, opportunities for recruitment and vetting, and migration hubs when platforms are dismantled.

The dynamism of forums' is well illustrated by users' migrations from legacy communities – such as **BreachForums** and **XSS**[3] – towards smaller, invitation-only spaces. When forums collapse, user migration is rapid, and new iterations or successor forums emerge within weeks, sometimes backed by the same core actors.

In 2025, **DarkForums** has emerged as the successor of BreachForums (read more in the cyber-attacks chapter), enabling the exchange of leaked data, sale of malware, and distribution of hacking tools across both its surface- and Tor-based platforms.

1.2 The criminal infrastructure: from residential proxy to proprietary hosting services

Modern threat actors rarely confine their operations to the dark web alone. Instead, they increasingly rely on a hybrid ecosystem of anonymity, which includes E2EE messaging platforms and decentralised protocols across both clear and dark web.

Bullet-proof hosting and layered anonymisation as persistent blockers

Cybercriminals continue to rely on BPH providers, which create resilience for their backend infrastructure. These services, sometimes embedded within multi-layered leasing arrangements (sub-sub-leasing) are nested across several jurisdictions, systematically disregarding abuse notifications and judicial takedown requests. Legal measures directed at these hosting providers often result in LEAs obtaining delayed or incomplete electronic evidence, due to limited data retention frameworks or redirection of the judicial requests to intermediaries.

Enhanced anonymisation methods, such as routing traffic through multiple VPN servers (VPN-chaining) and Tor nodes, are also increasingly observed. These techniques introduce successive layers of masked IPs, and possible encryption, before the traffic reaches the hosting environment, complicating source attribution and delaying the investigation due to numerous additional cross-border judicial requests.

Some criminal networks increasingly bypass third-party providers and deploy their own proprietary infrastructure. By owning the hardware, these groups effectively avoid localisation and seizure warrants.

Residential proxy services marketed to cybercriminals

The use of residential proxies in the cybercriminals' attack infrastructure helps camouflage their activity as legitimate traffic, making it harder for LEAs to detect, track and attribute malicious traffic routed through home-user IPs in different countries. Residential proxies act as intermediary servers, with an IP-address assigned to an internet-connected home device. They are widely available and marketed as a way to bypass geo-block or verifications, but these connections can be hijacked or rented by cybercriminals and used to disguise malicious traffic, launch DDoS attacks or scrape data.

Residential proxies can become compromised through vulnerabilities in the unpatched and/or unsecured home appliances or by installing malicious applications that grant access to the device. The proxy networks are easy to maintain - even following a disruption causing a proxy's unavailability, the vulnerability leveraged for the initial compromise is likely still present and may be exploited again, by a different actor, putting it back onto the criminal market.

DNS abuse: a critical delivery infrastructure for cyber-attacks and OFS

DNS abuse effectively bridges the gap between criminal infrastructure and victims of both OFS and cyber-attacks[4]. Technical DNS abuse and website content abuse are tightly intertwined in the criminal process. For instance, criminals register domains to harvest user credentials through imitations of legitimate websites (e.g. financial institutions).

Additionally, ransomware and malware operations abuse DNS for delivery and for Command and Control (C2) of botnets, leveraging residential proxies to anonymise traffic and impersonate legitimate users.

Criminal networks exploit efficiently the time period between domain registration and LE intervention. The absence of automated reporting interfaces and the reliance on slow, cross-border judicial assistance protocols prevent the mitigation (e.g. blocking or take-down of malicious domains) required to stop automated fraud and malware distribution campaigns before they reach scale.

1.3 Cryptocurrencies and other financial facilitators

The use of cryptocurrencies in cybercrime is evolving rapidly, adapting to advancements in blockchain technology, decentralisation, and anonymisation tools. Cryptocurrencies are used to conduct illicit activities through automated tools. They are no longer solely a cybercrime facilitator but now a well-established obfuscation means in the wider SOC landscape.

Privacy coins and off-shore exchange services make ransomware more sophisticated

In 2025, cryptocurrencies served as the preferred payment method for ransomware attacks, mainly due to their relative anonymity and borderless nature. Offenders have been increasingly utilising privacy coins, thanks to their built-in anonymity features, to further obfuscate the origins and destinations of their transactions. This shift highlights a growing trend towards high-opacity coins that are resistant to blockchain tracing tools, posing new challenges to LEAs. Criminals often favour the use of exchange services located in jurisdictions with loose anti-money laundering (AML) protocols or off-shore financial centres.

The growing popularity of cryptocurrencies broadens the target pool

Cryptocurrencies remained largely targeted in cyber-enabled fraud, as they are also becoming increasingly accessible to minors and young adults, also via social media 'get-rich' schemes, and for peer-to-peer trading. Having gained wider acceptance as a form of payment and investment, a sharp rise in crypto assets thefts has been reported in 2025 (read more in the section on cryptocurrency drainers). Minors may unknowingly engage in money laundering by renting out wallets or receiving crypto 'gifts' from cybercriminals.

Mixing-as-a-service for money laundering

One of the most significant trends for cybercriminal usage of cryptocurrencies in 2025 is **the rise of chain-hopping linked to money laundering (ML) operations**. With the advent of blockchain bridges, which facilitate the transfer of assets between blockchains, criminals can move funds rapidly across blockchains, further complicating the process of tracing illicit transactions. Bridging as such is a legitimate and essential technology in the cryptocurrency industry, serving as the 'connective tissue' that enables interoperability between otherwise isolated blockchain networks. Criminals would use a bridge to access opportunities on different chains without selling assets and paying exchange fees. Their speed, liquidity, and relative decentralised nature make them the preferred laundering method for ransomware actors and major dark web marketplace administrators.

The use of privacy coins remains popular among professional money launderers linked to ransomware operations, spoofing services and other forms of cybercrime, despite their declining use on centralised exchanges due to bans.

Especially for vendors on dark web marketplaces, 'coinjoin' services combining multiple coins from multiple users into a single transaction[I] remain a popular mixing solution (even if regulatory and enforcement pressure have increased following the

[I] CoinJoin is a privacy-focused technique used in cryptocurrency transactions to enhance anonymity. It works by combining multiple transactions from different users into a single transaction, making it difficult to trace the origin and destination of the funds. This process helps to break the link between the sender and receiver, thereby increasing privacy.

takedown of **cryptomixer.io**). As coinjoin services are rather 'slow' (a single mixing round can take an hour), users seeking speedy movement of illegal funds to an off-ramp[II] choose faster solutions, such as smart contract-based mixers (also known as 'mixer-as-a-service') and decentralised exchanges (DEXs). These services utilise automated market makers (AMMs) for instant settlement, eliminating the need for manual order book matching, middleman approval, or custodian delays. They operate directly on-chain, allowing for 24/7, peer-to-contract trading. The growing prevalence of such services has made the tracking of illicit transactions even more challenging for investigators, as these platforms bypass traditional financial institutions that enforce know your customer (KYC) and AML regulations.

EUROPOL AND PARTNERS SHUT DOWN CRYPTOMIXER

An illegal cryptocurrency mixing service called 'Cryptomixer' was suspected of facilitating cybercrime and money laundering. Cryptomixer was a hybrid mixing service, accessible via both clear and dark web. It facilitated the obfuscation of criminal funds for ransomware groups, dark web forums and markets. Its software blocked the traceability of funds on the blockchain, making it the platform of choice for cybercriminals seeking to launder illegal proceeds from a variety of criminal activities, such as drug trafficking, weapons trafficking, ransomware, and payment card fraud. Since its creation in 2016, over EUR 1.3 billion in Bitcoin were mixed through the service. In November 2025, Europol supported an action week conducted by LE in Switzerland and Germany in Zurich, Switzerland. Three servers were taken down and seized in Switzerland, along with the cryptomixer.io domain. The operation resulted in the confiscation of over 12 terabytes of data and more than EUR 25 million worth in cryptocurrencies[5].

Other fintech services such as pre-paid cryptocurrency credit cards provide off-ramp services to integrate illicit funds into licit financial flows, bypassing EU AML rules. Cryptocurrency-to-cash desks remain a critical physical service where digital theft is converted into fiat currency. This dual evolution in both physical and digital vectors, the latter all accessible via smartphone, contribute to the further diversification of channels for money laundering and criminal finance, making illicit financial flows increasingly difficult to trace.

1.4 Automation and AI

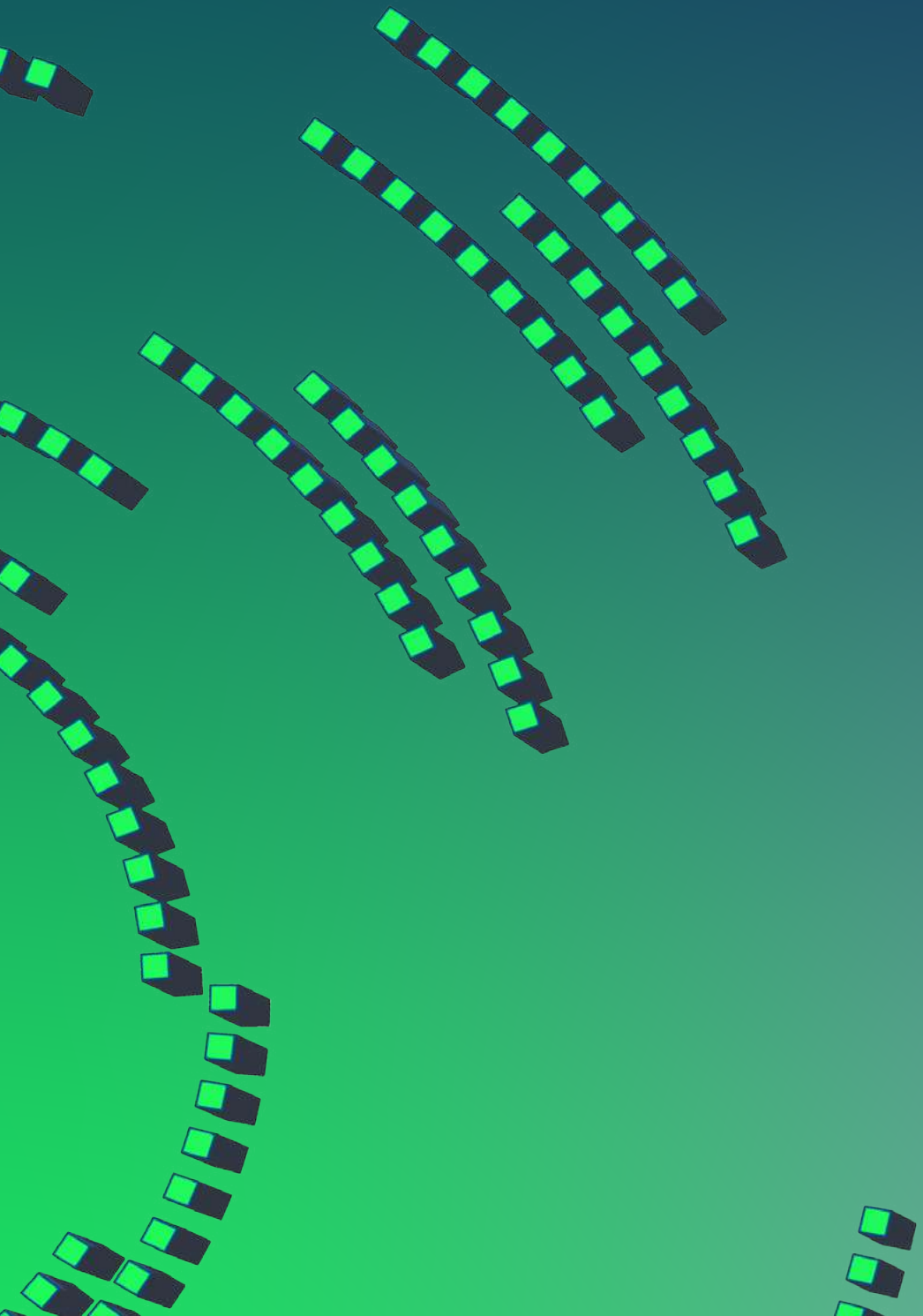
The rapid evolution and accessibility of a wide range of AI tools continuously create opportunities for the whole cybercrime ecosystem to increase efficiency, speed and reach. Criminal networks involved in cybercrime adeptly harness AI and automation to upscale their operations, facilitated by the parallel integration of AI capabilities in legitimate security contexts and business applications, which opens further avenues for exploitation.

Transnational communities of child sexual exploitation (CSE) offenders, fraud networks, and ransomware groups are constantly working to expand their operational capabilities and operational security through the use of generative AI tools and automated bots. Cybercriminals also take advantage of legitimate commercial applications using AI technology.

The dark web remains an important hub for malicious large language models (LLMs), which are built or adapted to remove ethical constraints and filters from legitimate commercial solutions[6]. AI models can also be tailored for criminal purposes by providing inputs that are most relevant and accurate for that application. For example, malware samples, guides on how to carry out OFS or how to set up infrastructure not to be detected and identified can be used to improve the precision and quality of the malicious output of the model.

[II] Crypto on-ramps and crypto off-ramps are services that allow users to exchange fiat currency — government-issued money — for cryptocurrencies, and vice versa. They connect bank accounts, payment cards and digital wallets to crypto exchanges or platforms, so people can buy, sell or spend digital assets securely and easily.

THE CRIMINAL INFRASTRUCTURE BEHIND ONLINE FRAUD SCHEMES



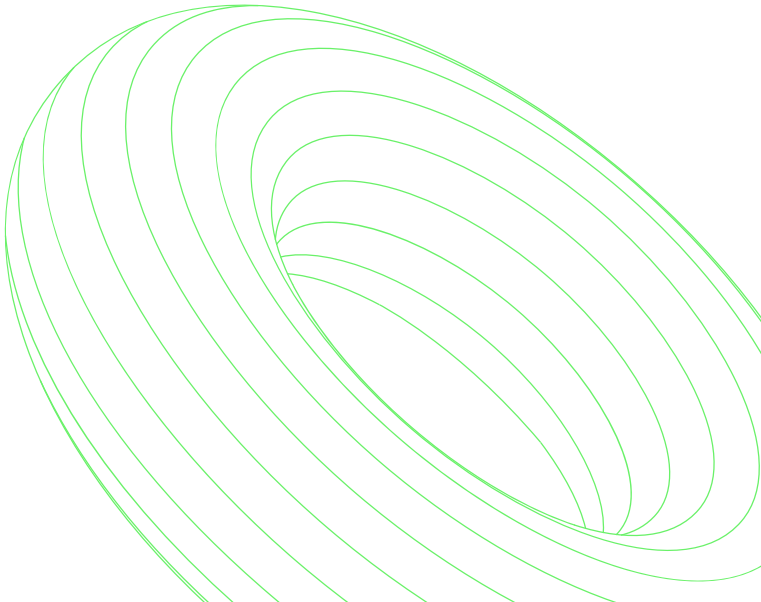
02

Key Developments

- The threat from online fraud schemes continues to grow, supported by a criminal infrastructure enabling speed, industrial-scale victimisation and increased anonymity. Online fraud schemes commonly involve phishing, with malicious advertising as a popular attack vector, enabling the targeting of victims with precision. The abuse of SIM boxes provides hardware for large-scale attacks.
- Certain criminal networks have shifted away from using commercial bulletproof hosting and instead have started to deploy their own infrastructure, so as to bypass KYC protocols and disrupt traditional evidence chains.
- The theft of digital assets via cryptocurrency drainers has matured to a crime-as-a-service (CaaS) system, driven by the uptake of DeFi across the EU, their growing popularity for money laundering purposes, as well as a rising diversity in digital assets available.
- While fraudsters' use of generative AI has improved their ability to personalise social engineering techniques, the criminal adoption of agentic AI to automate parts of the criminal process is set to raise the threat from OFS to unprecedented levels.

Fraud schemes represent the fastest-growing area of organised crime. Fraudsters generate large profits by targeting individuals, public and private sector organisations, and their data. Investment fraud (especially crypto), business email compromise (BEC), romance, tech support and fraud against payment systems are the most common OFS typologies reported by Member States.

While sophistication of techniques and modi operandi vary, cybercriminal networks are particularly active in fraud against payment systems, aimed either at stealing funds or at obtaining personal information[7]. Stolen data are not just used for the fraud scheme but often sold onwards and further exploited by other criminals, via clear and dark web, in a vicious loop where targets are relentlessly re-victimised.



2.1 OFS threat becomes faster and more concealed

Law enforcement reporting throughout 2025 indicated a transition from a threat landscape largely defined by volume and variety of fraud schemes to one also characterised by velocity and more complex operational security.

The adoption of technological advancements allowed OFS to evolve into a high-speed and borderless AI-leveraged criminal activity. Generative AI continued to accelerate online fraud, enabling criminal networks operating from outside the EU to personalise narratives with ease and target EU citizens at high speed and vast scale. This is exemplified in AI-assisted impersonation (e.g. of bank helpdesk or law enforcement personnel), and enhanced realism in business email compromise (BEC) and CEO fraud.

By advertising on very large online platforms (VLOPs)[8], criminal networks can industrialise victims' targeting and bypass geographic or linguistic barriers, a significant enabler especially for crypto investment fraud, now largely happening on VLOPs.

SIM boxes: The industry-like system

The use of SIM boxes to enable fraud has further globalised, with this technology internationally sourced by criminal networks targeting the EU. These farms can provide mass-scale anonymity for phishing campaigns, allowing criminal networks to bypass KYC protocols and subscribe to thousands of services simultaneously – including fraudulent advertising platforms and fake accounts for social media and communication applications. Fraudulent platforms and accounts can be localised to the targeted country, concealing the fraudsters' identity and location.

A **SIM box** is a device that houses hundreds of SIM cards used as part of a voice-over-IP gateway installation. Criminals use them to mask communication data and to make calls or send SMS messages at cheaper rates. A group of SIM boxes is known as **SIM farm**. SIM farms can facilitate the dissemination of thousands of SMS, calls and social media posts to enable large-scale fraud.

Active farms have been identified in the EU and are often utilised remotely by criminal networks based in other jurisdictions. The global reach of these anonymity services illustrates that the SIM box ecosystem is a cohesive, transnational supply chain rather than a localised threat.

Criminal associates travel to jurisdictions where SIM bulk purchasing is possible and registration is either not necessary or less regulated. These assets are then physically trafficked to hosting locations, to populate the industrial-scale SIM farms that nowadays underpin the majority of online fraud operations. This illustrates criminal reliance on a dedicated physical supply chain that law enforcement can intercept.

CAAS NETWORK PROVIDING SIM BOXES FOR TELECOMMUNICATIONS-ENABLED CYBERCRIMES

A network of seven Latvian nationals had set up a SIM farm used to enable crimes against thousands of victims across Europe. The infrastructure comprised at least 1 200 SIM-box devices, operating 40 000 SIM cards linked to telephone numbers registered to people from over 80 countries around the world, offered for criminal abuse. Most fraud schemes using this service involved phishing to gain access to victims' e-mail and banking accounts. While the true scale of this network is still being uncovered, more than 49 million online accounts were created on the basis of the illegal service provided by suspects. Offences facilitated by this criminal service included various forms of online fraud, but also extortion, migrant smuggling and the distribution of child sexual abuse material. The damage caused to victims amounts to millions of Euros. Austrian, Estonian, Latvian, and Finnish authorities, supported by Eurojust and Europol, arrested the group in October 2025[9].

FIGURE 1 - SIM BOXES AND SIM CARDS SEIZED DURING THE OPERATION

IMSI catchers: an interception technology used for OFS

While CaaS and technology advancements continue to lower entry barriers for scammers, the primary operational evolution is the deployment of more sophisticated telecommunications infrastructure, to bypass KYC protocols and disrupt traditional evidence chains, as commonly seen in phishing and account takeover (ATO) campaigns.

A rise in the use of IMSI catchers (and SMS blasters, also enabled to send SMS messages) points to the adoption of interception technology by criminal networks.

An **IMSI catcher** is a device that mimics a cell tower, broadcasting signals to make mobile phones in its range connect to it, thus enabling the harvesting of personal and sensitive data. Devices that also have the capability to send SMS messages, are referred to as **SMS blasters**.

Since the connection is downgraded to 2G, these attacks can occur 'under the radar' of commercial telecommunication providers – effectively bypassing the legitimate network, thus allowing criminals to avoid attribution and disrupt traditional evidence chains.

2.2 Relay attacks

Relay attacks on payment terminals increased in the EU throughout 2025[10], specifically terminal-to-terminal and card-to-terminal vectors (see figure 2). In a terminal-to-terminal relay attack, transaction data is transferred in real-time between a payment card (or digital wallet) and a relay device in possession of the criminal to enable cash-out[11]. In a card-to-terminal relay attack, the victim is deceived into installing a malicious app and insert card details and PIN, which are then used by criminals to cash out.

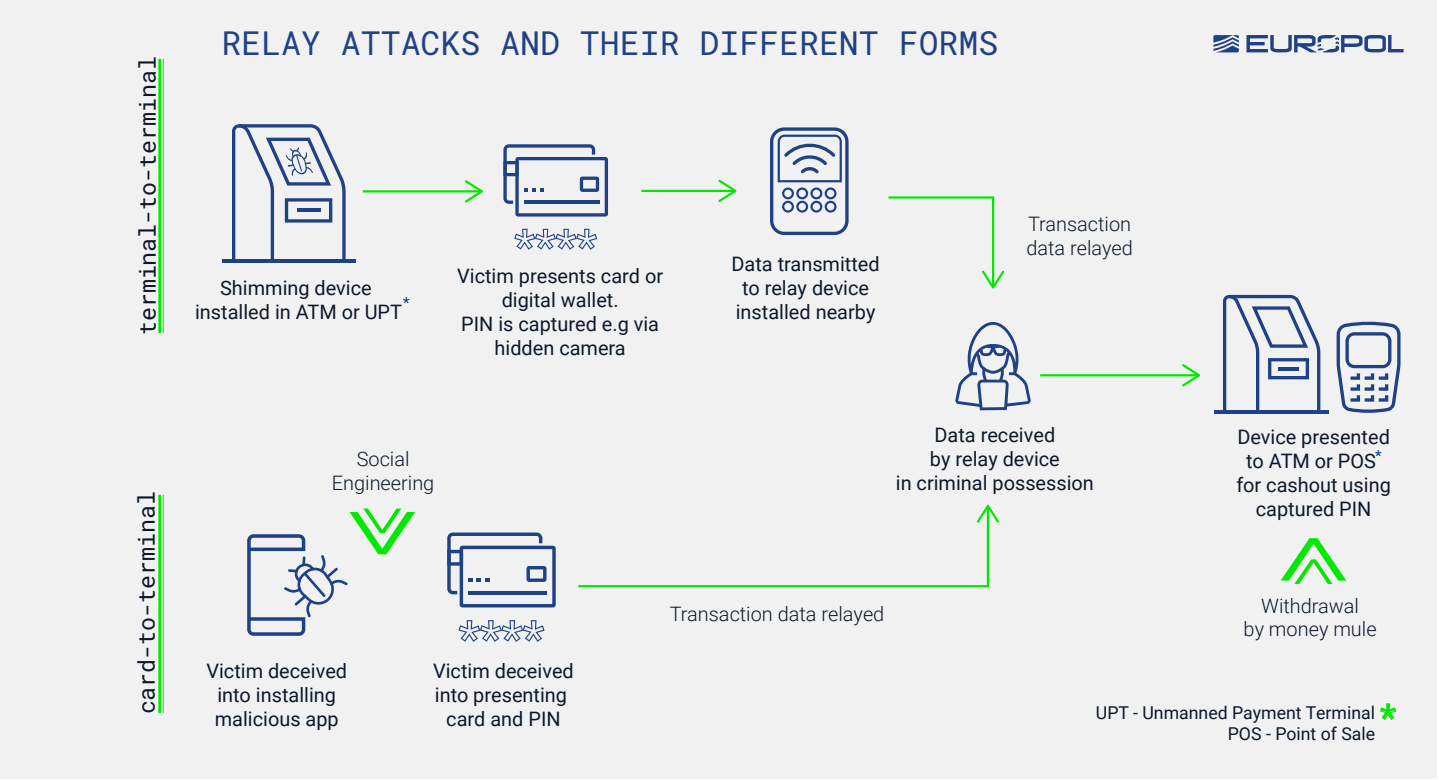


FIGURE 2 - SIMPLIFIED OVERVIEW OF RELAY ATTACKS AND THEIR DIFFERENT FORMS: TERMINAL-TO-TERMINAL AND CARD-TO-TERMINAL [SOURCE: EUROPOL]

2.3 Digital asset theft via cryptocurrency drainers

Theft of digital assets via cryptocurrency drainers kept fluctuating throughout the year, due to a volatile cryptocurrencies market and subsequent user activity, as well changes in the criminal landscape (i.e. the acquisition of a large crypto wallet draining service, Inferno Drainer, by a rival draining-as-a-service provider, Angel Drainer, in October 2024)[12].

Cryptocurrency drainers are specialised malwares that target the Web3 ecosystem[I], designed to grant attackers unauthorised control over victims' wallets. The attack vector relies heavily on phishing and social engineering; victims are manipulated into connecting their wallets to malicious smart contracts and unknowingly approving transactions that authorise the immediate draining of their funds. This threat has matured into a CaaS system.

It is plausible that cryptocurrency drainers are also used by hybrid-actor-linked criminal networks. The threat may continue to expand in line with increasing public uptake of cryptocurrencies and the utility of these assets for laundering criminal proceeds.

[I] Web3, short for Web 3.0, refers to the newer generation of the internet, more decentralised, open, and user-controlled compared to the Web 2.0. Web3 leverages privacy-reducing technologies like blockchain, smart contracts, DeFi, NFTs, etc.

2.4 OFS networks rely on a wide range of enablers

The smartphone is the essential common denominator in modern OFS developments, functioning not merely as a communication tool but as the primary means to circumvent KYC checks. While caller ID spoofing[II] continues to be a major enabler for fraud, online fraudsters have learned to abuse the rapid customer onboarding business model of neo-banks[13]. They enable the fast registration of a continuous stream of new accounts and customers, which places pressure on KYC mechanisms.

Parallel to this increased reliance on mobile identity and financial services, some criminal networks involved in OFS have moved away from commercial bulletproof hosting and are increasingly deploying their own infrastructure[14]. This shift represents a countermeasure against LE access to backend data (read more in the Cybercrime enablers chapter).

Infrastructure for anonymisation via virtual computers has also been incorporated into the extensive CaaS ecosystem supporting online fraud. Criminal marketplaces offering virtual desktop services (VDS)[III] allow fraudsters to enjoy full administrative control and no usage limits, while enhancing anonymisation and enabling location spoofing.

Malicious advertising (also called malvertising) is another primary enabler of high-volume and large-scale fraud, especially relevant in crypto-investment fraud schemes. Criminal affiliate marketeers abuse VLOPs and legitimate marketing platforms to cater to fraudsters huge volumes of victims, behind a façade of legitimacy.

Malvertising ranges from advertisement of fraudulent websites or mobile applications that imitate legitimate banking, investment or trading platforms, to fake accommodation or merchandise listings. Unlike banks, which face license revocation for facilitating financial crime, major tech platforms currently lack comparable penalties to report fraudulent advertising effectively[IV].

The prominence of phishing and smishing campaigns is a direct adaptation to the EU shift towards two-factor authentication (2FA). Despite EU regulations[V] on 2FA[15], and with biometric authentication (e.g. face, fingerprint and iris identification) becoming increasingly commonplace, criminals will continue to seek technical ways to bypass these protocols. However, social engineering and human error will remain the weakest links for fraudsters to exploit.

While the deployment of agentic AI — systems capable of autonomous operational planning and execution — remains a developing driver for crime, criminal networks continue to effectively utilise generative AI to upscale their operations. Artificial Intelligence support includes coding assistance and generation of conversation scripts, to aid call centre operators.

Voice chat bots are also increasingly deployed to pre-screen victims at industrial volume, acting as a filter for human operators, thereby significantly increasing the efficiency of fraud centres. However, industry intelligence reveals that this adoption comes with vulnerabilities; criminals frequently rely on public, jailbroken LLMs.

II Caller ID spoofing is a technique used to falsify the information transmitted to the caller ID display in order to disguise the caller identity. Caller ID spoofing usually happens on traditional landline phones, mobile phones, and Voice over Internet Protocol (VoIP) systems.

III A virtual desktop service, sometimes called Virtual Desktop Infrastructure (VDI) or Desktop-as-a-Service (DaaS), allows users to access a desktop environment and its applications from anywhere, using any device with an internet connection. Instead of running applications on a local device, the applications run on a remote server, and the user interacts with them through a virtual desktop interface.

IV Despite the enforcement framework under the Digital Services Act (DSA), including fines for Very Large Online Platform (VLOP) of up to 6% of the global turnover; European Commission, 2025, The enforcement framework under the Digital Services Act, accessible at https://digital-strategy.ec.europa.eu/en/policies/dsa-enforcement.

V Including the eIDAS Regulation and Payment Services Directive 2 (PSD2).

CYBER-ATTACKS

03

Key Developments

- The ransomware landscape remains highly volatile and fragmented due to an increasing number of emerging ransomware brands, driven by competition among criminal actors, the aftermath of LE actions and new available technological resources. In 2025, Europol observed more than 120 active ransomware brands, with ransomware attacks steadily increasing.
- Ransomware-as-a-service (RaaS) groups are increasingly seeking to broaden their service offerings to attract affiliates, including through functionalities leveraging AI tools and more customisable branding.
- There are noticeable overlaps across different ransomware operations and brands and the affiliates and administrators involved, showing their significant role in the ransomware ecosystem.
- Hybrid threat actors leverage cybercriminal networks as proxies for destabilisation purposes, through DDoS or ransomware attacks, for data theft operations and to compromise strategic targets.

3.1 An increasingly interwoven ecosystem

Ransomware persists as a key threat in the EU, with a significant number of ransomware families[I] active throughout 2025. Criminal actors continued leveraging vulnerabilities and targeted the digital supply chain to scale their attacks and deploy increasingly sophisticated social engineering techniques. The focus of the extortion has shifted from releasing (decrypting) the data to pressuring victims to pay for it to not be released (leaked), showing the importance of data in today's digital economy.

While financial gain remains the dominant motivation behind cyber-attacks, the relationships between state hybrid threat and criminal actors have become more and more interwoven. Hybrid threat actors use cybercriminal networks as proxies for interference activities, which include DDoS attacks, intrusions, data theft operations and ransomware attacks. Cybercriminals may serve as proxies unknowingly, others in exchange for protection from prosecution or under coercion[16]. In the prevailing CaaS cybercrime economy, hybrid threat actors just become customers among other customers.

Ransomware: brands fragmentation and short-lived operations

In 2025, Europol observed more than 120 active ransomware brands, with ransomware attacks steadily increasing. The ransomware environment continues to be highly unstable and divided, fuelled by a growing number of new brands, rivalry among criminals, the consequences of LEAs interventions, and the availability of new technological tools.

[I] A ransomware family refers to ransomware samples sharing a common codebase, encryption method, or functional characteristics. A brand is the name adopted by the cybercriminals, like a label chosen to be identified behind attacks/services/tools.

Many **ransomware operations** continue to be short-lived and more likely to rebrand within a shorter timeframe, with a noticeable overlap of administrators and affiliates involved and between different ransomware groups' attack, proxy and money laundering (ML) infrastructure. Ransomware operators can easily pivot their activities, increasingly thanks to the abundance of available leaked ransomware codebases, AI-powered code-assembly tools and RaaS platforms enabling the creation by other criminals of their own malware version.

Initial access is acquired in various ways, with the method of choice usually dependent on the ransomware operator's skills and preferences. Common attack vectors include phishing, infostealers, exploiting unpatched vulnerabilities in public-facing applications, via Initial Access Brokers (IABs), and/or insider threats[17] continued to be deployed.

Multi-layered extortion tactics focus on threat of data release

Most ransomware groups still deploy multi-layered extortion tactics, with data exfiltration as a key element of coercion. Many victims are more willing to pay for their data *not* to be released (publicly leaked), in contrast to the early days of ransomware, when the extortion focused on the need of the victim for the data *to be* released (i.e. decrypted) back to them. Modern enterprises are generally more prepared to deal with the impact of data being lost (encrypted or erased), compared to being published. Simultaneous DDoS attacks, spamming of corporate email addresses and psychological pressure via cold-calling are common in the extortion toolkit of ransomware actors, and are sometimes offered as a service.

3.2 Main developments in the ransomware ecosystem

Ransomware groups vary according to their barrier to entry, their technical sophistication as well as their motivation (i.e. financial, ideological or both). They generally divide in three main groupings: public affiliate programs, semi-closed and closed groups.

Public RaaS affiliate programs

Public RaaS affiliate programs allow almost anyone to sign up and carry out attacks using the different capabilities integrated into their platform. In addition to the malware assembler, these can include botnets for pay-load distribution, tools for persistence and victim monitoring, data exfiltration and ML infrastructure, services for ransom negotiation and leak-site hosting. The administrators of the platform take a percentage of each ransom payment facilitated through their service.

Running exfiltration-focused infrastructure and data leak sites is highly resource-intensive, which is why cybercriminals turn to RaaS platforms. RaaS providers, in turn, are incentivised to offer convenient all-in-one solutions to attract affiliates and establish a reputable and stable brand-identity.

Qilin emerged as a dominant ransomware family in 2025. It offers its affiliates a comprehensive toolkit and have recently included integrated DDoS capabilities to pressure victims[18]. The group seems to be working on automating attack-based vulnerabilities in Fortinet Secure Socket Layer (SSL) VPN devices, thus enabling affiliates to launch attacks on desired targets. The core group appears to be based in Russia, with ties to the defunct Conti group. They present themselves as an ideologically motivated group, although activity appears financially driven and they offer one of the highest affiliate profit-shares in the market (80 % - 85 % of the ransom payment)[II].

[II] A Secure Socket Layer protocol enables remote users to securely access corporate network resources using either a web browser (web mode) or the FortiClient device, which provides full network access.

Akira, also with ties to Conti, is operating since March 2023 and has maintained significant activity in 2025. There are overlaps in the codebase used by both groups as well as the crypto-wallet addresses used by their affiliates. In 2025, Akira also expanded their capabilities to target virtualised infrastructure, likely by leveraging SonicWall[III] vulnerabilities for initial access[19].

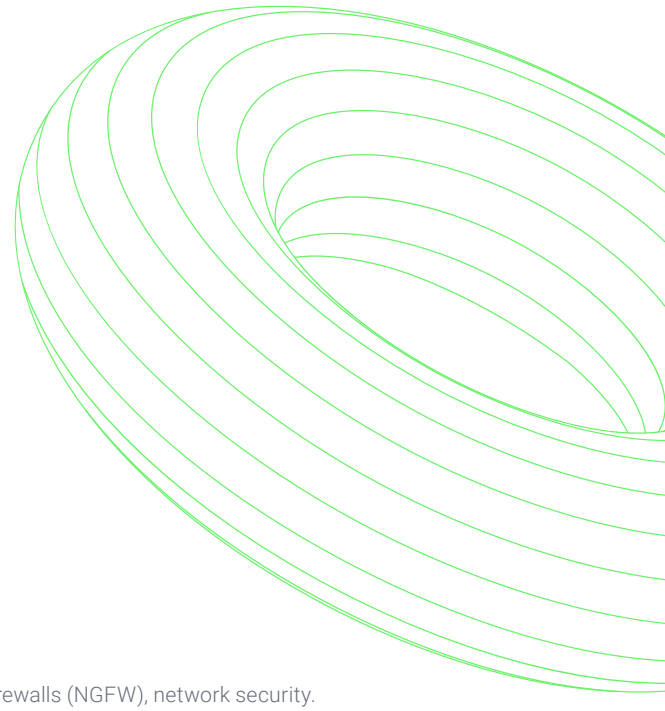
Following its takedown in 2024[20], **LockBit** has made several attempts to rebound in 2025, although with limited success. In May, LockBit suffered a data breach resulting in builds, build configurations and victim negotiation messages being leaked[21]. Since then, its activity dwindled and the number of victims significantly decreased. LockBit 5.0 was released in September, including variants capable of targeting Windows, Linux and VMware. They have updated anti-forensic mechanisms, faster encryption routines, geolocation checks to avoid infecting Russian-language systems, and other features that complicate recovery. The new version is accessible for a little over EUR 400 (USD 500)[22].

DragonForce, a largely Russian-speaking group active since 2023, stood out in 2025 with a novel business model, capabilities and competitive approach[IV]. DragonForce offers different payloads, assembled from Conti and LockBit leaked codebases, and allows affiliates to build different variants for targeting Windows, Linux, VMware and other platforms. In August, a new extortion service was announced, offering exfiltrated data analysis and the creation of tailored extortion materials (e.g. call scripts, draft letters and advice reports), to maximise the pressure on victims. The service fees can be over 20 % of the ransom payment and it is mainly marketed to affiliates targeting high-revenue organisations[23].

In September 2025, a new coalition between DragonForce, LockBit and Qilin was announced on the dark web.

PHOBOS AND 8BASE DISRUPTION[24]

Phobos had been a long-standing RaaS provider with a particularly accessible and adaptable platform, allowing customisation of ransomware campaigns with minimal technical expertise. Taking advantage of the Phobos infrastructure, 8Base developed its own variant. This group had been particularly aggressive in its double extortion tactics, not only encrypting victims' data but also threatening to publish stolen information unless a ransom was paid. Phobos and 8Base declined in activity in 2025, following coordinated international LE actions supported by Europol and the arrests of four individuals of Russian nationality. As a result of this operation, law enforcement was also able to warn more than 400 companies worldwide of ongoing or imminent ransomware attacks.



[III] SonicWall is a cybersecurity company specialised in next-generation firewalls (NGFW), network security.

[IV] Its disputes with the now disbanded RansomHub group saw their leak site being taken out in March 2025 and apparently not having returned by the end of 2025.

Semi-closed groups

Semi-closed affiliate programs are more selective and likely to carry out targeted recruitment on cybercriminal platforms. The core group, made of developers and administrators, seek out skilled, trustworthy and ideologically aligned affiliates to carry out attacks using their platform.

Fog, a ransomware first detected in early 2024, has a modular design, allowing attackers to control the targets and scope of the encryption, content of the ransom note and other aspects of the attack. The group also has a dedicated leaks site and negotiation portal to communicate to victims. Currently it can be classified as a semi-closed group, with operators using shared infrastructure and tactics, techniques, and procedures (TTPs).

BlackBasta was a Russian-speaking group with also roots in Conti[25] that generally used spear-phishing or exploitation of known vulnerabilities to gain access to victims' networks. In 2025, BlackBasta suffered a leak of its internal chat logs, containing a wide range of information, such as phishing templates, cryptocurrency addresses and victims' credentials[26]. The groups leak sites are inactive, but the criminal actors related to BlackBasta are likely to continue their activities under a different brand.

Closed groups

Closed ransomware groups consist of criminal actors who have likely worked together for years and operate with less dependence on CaaS. They develop their own malware and sometimes exploits, use closed communication channels, host much of their own infrastructure, and carry out the attacks themselves. These groups are usually sophisticated and more resilient. As they do not rely on as many commercial criminal services, their identification is more difficult, because their traces are less likely to appear in seized or leaked datasets. They maintain a high level of operational security, and foster stronger trust within their inner circle, further reducing the risk of exposure.

Cl0p is a longstanding closed group known for systematically exploiting zero-day vulnerabilities[27], which resurfaced in February 2025 after a period inactivity.

Play (also known as PlayCrypt) ransomware group continued to be active in 2025. The group has previously targeted critical infrastructure and continues deploying double extortion tactic, with a claimed guarantee on the secrecy of deals[28].

3.3 New hacking coalitions threaten big tech and customer data

In August 2025, the alleged **Scattered LAPSUS$ Hunters (SLSH)** alliance emerged, between Scattered Spider, ShinyHunters and LAPSUS$ hacking collectives. These mostly English-speaking collectives have previously been involved in a range of cybercriminal activities, including online fraud and SIM swapping, high-profile social engineering, insider threat recruitment, data theft and extortion campaigns against major corporations, healthcare and transport providers.

The potential threat of this new coalition is significant, considering the capabilities of the groups' members demonstrated in previous attacks. There are also reports of SLSH members' use of continues harassment and threats, which are not guaranteed to stop even after victims' ransom payments[29]. Some members of the three groups also appear to be tied to E2EE channels used by The Com network, engaged in real-life violence, CSE and violent extremism, which further indicates the fluidity between online criminal communities (read more in the chapter on Child Sexual Exploitation)[30].

Scattered Spider emerged around 2022 and became known for their high-profile social engineering attacks used to infiltrate corporate networks and extorting their victims, as well as online fraud and SIM-swapping activities. In 2023, Scattered Spider members claimed to have acted as an initial access broker (IAB) against UK and US corporations via the ALPHV/BlackCat ransomware affiliate group. The group was also responsible for the cyber-attack against Transport for London in 2024, as well as for extorting many UK retail and US healthcare providers[31].

LAPSUS$ started their activities in 2021 as a small but notorious extortion-focused group that used spear-phishing, SIM-swapping and insider recruitment techniques to breach major tech firms like Microsoft, Samsung NVIDIA, Okta, T-Mobile, Uber, Rockstar Games and many others[32]. In 2022, several members were arrested by the City of London Police in connection to these attacks, which led to the group going dormant.

ShinyHunters is known for their large-scale data theft and extortion campaign against major tech companies. In May 2025, ShinyHunters launched a social engineering campaign that siphoned over a billion Salesforce customer records by tricking victims to connect a malicious app to their organisation's Salesforce portal[33].

3.4 Infostealers continue to cater for the cybercrime market

Infostealers persisted as a key enabler for the entire spectrum of cyber-attacks in 2025. Infostealers cater to a broad illicit market of cybercriminals ranging from IABs and ransomware affiliates to fraudsters[34].

TARGETING CYBERCRIMINAL ENABLERS THROUGH GLOBAL PARTNERSHIPS

Continued iterations of the Europol-coordinated operation Endgame successfully disrupted infrastructure and criminal actors in the CaaS environment. This included the Smokeloader botnet[35], which was run as a pay-per-install service and enabled criminals to access to victims' machines for illicit activities, ranging from keylogging to the deployment of ransomware and cryptominers.

Another action in May, targeting initial access malware services, dismantled Bumblebee, Lactrodectus, Qakbot, Hijackloader, DanaBot, Trickbot and Warmcookie malware strains[36]. Around 300 servers were taken down worldwide, 650 domains neutralised, and international arrest warrants issued against 20 targets.

In November, Endgame targeted infostealers Rhadamantys, VenomRAT and the Elysium botnet. More than 1 000 servers worldwide were taken down or disrupted and the main suspect behind VenomRAT arrested in Greece[37]. The dismantled malware infrastructure consisted of hundreds of thousands of infected computers containing millions of stolen credentials.

The success of LEAs actions against key enablers also relies on contributions from the private sector, providing technical support to the takedown, as well as infrastructure identification and mapping.

3.5 DDoS attacks pose a hybrid threat

Sustained by the wide availability of modular stressor and booter service[V] offerings, DDoS attacks remain a threat. They are often state-sponsored and driven by ideological motivation[38], but also deployed as a means to extort victims or undermine competitors in the criminal ecosystem[39]. Targets include governments, critical infrastructure and high-impact economic sectors. While effective mitigation measures are generally in place and the impact is often low, the relatively minimal effort needed to launch this kind of attacks makes it an effective and sustainable strategy for continuous destabilisation.

DDoS attacks carried out in connection with global events of political significance, such as the June 2025 NATO Summit[VI], contributed to instil a sense of insecurity in society and undermine public confidence in institutions.

[V] Tools designed to test the stress resistance of a network to see if the resources designated to it (e.g. bandwidth, CPU) can withstand additional load.

[VI] During the 2025 NATO Summit, held in The Hague, Netherlands on 24-26 June 2025, several entities experienced DDoS attacks, including websites of summit side events, international organisations, regional transport companies, platforms used for public announcements by regional Dutch authorities and the municipality of The Hague. More information available at https://www.ncsc.nl/waarschuwing/ddos-aanvallen-op-nederlandse-organisaties-rondom-navo-top-0 ; https://www.icc-cpi.int/news/icc-detects-and-contains-new-sophisticated-cyber-security-incident

PRO-RUSSIAN CYBERCRIME NETWORK NONAME057(16)

Mainly Russian-speaking, a network called NoName057(16) known to be targeting governments and corporations, was operating around a core group of individuals based in Russia, with several followers not necessarily technically skilled and located in various countries, including the EU.

In July 2025, as part of Operation Eastwood, coordinated by Europol and Eurojust, and supported by ENISA, the infrastructure of the network was disrupted, followed by a number of international arrests[40]. The countries involved were Belgium, Canada, Czechia, Denmark, Estonia, Finland, France, Germany, Italy, Latvia, Lithuania, Netherlands, Poland, Romania, Spain, Sweden, Switzerland, Ukraine, and the United States.

Following the disruption of the network infrastructure, a decline in activity of the NoName057(16) was initially seen, however capability was quickly recovered and their activity resumed. More recently, the group appears to be moving towards exploring and more impactful attacks, including against industrial control systems.

NONAME057(16) OPERATION **EASTWOOD**

WHAT CRIMINAL ACTIVITIES ARE WE STOPPING?

This operation targeted the criminal network NoName057(16), linked to **73** DDoS attacks per day of Ukrainian private and public actors.

6032 < UNIQUE HOSTS ATTACKED />

674 < PUBLIC WEBSITES ATTACKED />

5358 < PRIVATE WEBSITES ATTACKED />

19 < COUNTRIES INVOLVED />

200 < POLICE OFFICERS INVOLVED />

24 < HOUSE SEARCHES />

+100 < SERVERS DISRUPTED WORLDWIDE />

9 < ARRESTS WARRANTS ISSUED, 2 OF THEM EXECUTED />

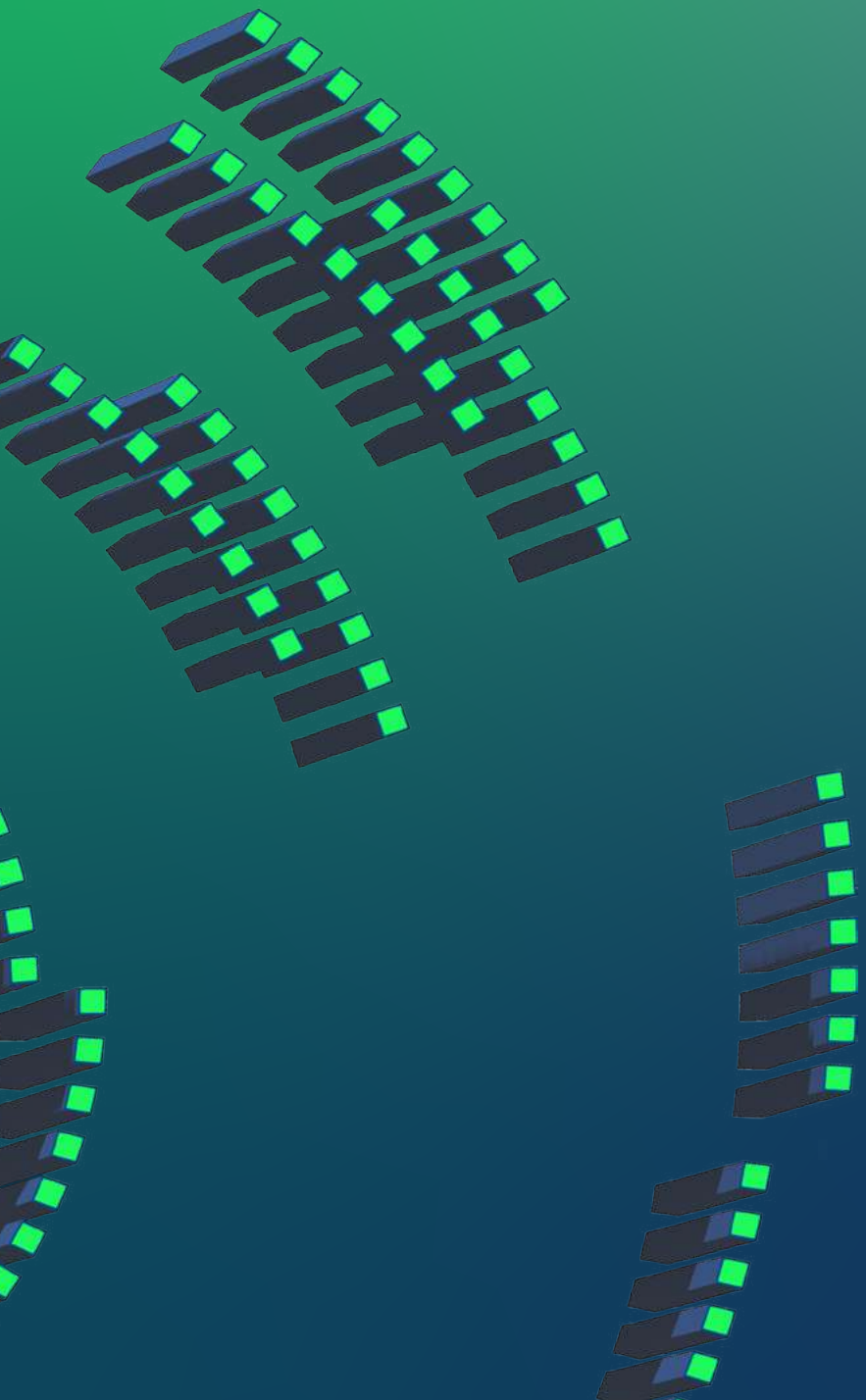
5 < EU MOST WANTED />

13 < INDIVIDUALS QUESTIONED />

+1000 < SUPPORTERS NOTIFIED FOR THEIR LEGAL LIABILITY />

< MAIN INFRASTRUCTURE TAKEN OFFLINE />

ONLINE CHILD SEXUAL EXPLOITATION



04

Key Developments

- Extortion remains a key threat linked to CSE, with child victims manipulated into sending money, producing more sexual content and committing violent acts, including self-harm, to comply to the demands.
- Trade in child sexual abuse material (CSAM) for financial gain is increasing. While live-distant child abuse (LDCA) remains a persistent threat, financial sexual extortion continues to surge. More platforms selling CSAM are identified, along with scam sites related to the sale of CSAM.
- AI-generated CSAM is increasingly being detected, creating additional difficulties in the analysis of CSAM, victim identification, investigative capacity as well as regulatory challenges.
- E2EE messaging applications have become a prominent communication environment for CSE offenders, for grooming, exchange of CSAM, communication and networking, as they are fully aware of the difficulties that LEAs have in obtaining the data exchanged via these applications.

The evolution of the threat posed by CSE continued to be influenced by technological advancements. Offenders show exceptionally quick adaptation to new technologies, both to expand and make more efficient the criminal process, but also as a countermeasure against LE detection.

4.1 Sexual extortion cases continue to spike

Sexual extortion continues to be a major threat linked to CSE. It takes place in many shapes and it is perpetrated by several types of offenders who are moved by different motives, targeting an ever-increasing number of underage victims, with extremely serious consequences.

In 2025, the online distribution of self-generated sexual material from children continued to be a cause of concern. Even when it is not the result of a criminal process of manipulation, it often leads to several forms of CSE. Once the image is shared, the child depicted loses control over it and it can be re-distributed, traded, manipulated or posted on CSE platforms, with the risk to remain online for years. Such images are also often weaponised against the child and used as a leverage for sexual extortion, aiming either at sharing more explicit pictures or at obtaining money (financial extortion).

Both the amount of self-generated sexual images circulating online and the number of sexual extortion cases reported are constantly spiking in volume. Similar to previous years, the number of CyberTips reports related to financial extortion received by NCMEC between January and June 2025 increased by about 70%[I] in comparison with the same period the year before[41]. Such offences have serious consequences in children who are pressured psychologically and financially, with demands in many cases persisting also after demands are met. This process strongly impacts children who feel overwhelmed, ashamed and scared, and often do not seek for help.

[I] The number of reports went from 13 842 in the first six months of 2024 compared to 23 593 in 2025.

PREVENTION AND SUPPORT FOR VICTIMS: HELP4U[42]

Prevention and support for victims are key to mitigate online sexual abuse and CSE. Help4U is a digital platform created by Europol and the research centre CENTRIC to support children and teenagers who are facing online sexual abuse or other harmful online behaviour. It was launched in November 2025 as part of Europol's broader public-awareness and victim-support work on online child sexual exploitation.

Help4U is designed mainly for minors who feel unsafe online, for example because someone is pressuring them for sexual content, sharing their images without consent, or otherwise abusing them. Minors can use it to find local support services, get guidance in private at their own pace, and, in some countries, connect with professionals who can listen and help them move towards safety and recovery. It centralises trusted information on rights, online safety, and practical next steps (such as preserving evidence, blocking/reporting offenders, and seeking help) in clear, age-appropriate language. The platform also provides tailored information for parents, teachers, and other professionals who support young people affected by online sexual exploitation.

Help4U began as a pilot project between Belgium, Germany, Ireland, the Netherlands and Slovenia, and now includes Bulgaria, Croatia, Cyprus, Greece, Hungary, Italy, Portugal, Spain and Romania, with more countries expected to join in 2026.

4.2 Shifting offender behaviour: monetisation of CSAM

Networking, coordination and CSAM exchange among CSE offenders have traditionally relied on trust-based relationships. As a form of countermeasure against LE detection and social stigma, perpetrators tend to form relatively closed, reputation-driven communities where access and exchange are governed by social ties, status, and long-term interaction. This applies mostly for offenders driven by sexual interest towards children, while a minority of perpetrators have been carrying out and/or facilitating CSE offences operating in an opportunistic way, driven by financial gain.

Nevertheless, a significant shift towards CSAM monetisation appears to be influencing also offenders' behaviour, as CSE offenders are not anymore operating only within trusted circles and new types of offences and infrastructure continue to emerge.

Several new platforms selling CSAM have been identified and investigated throughout 2025. Many of the platforms advertised as solely dedicated to the sale of CSAM appear to be OFS sites. Users are able to access only content previews of CSAM or a limited amount of CSAM freely available on the site front page, while an upfront payment (usually in cryptocurrency) supposedly provides access to exclusive content. Once the user pays or submits the CSAM, they do not receive anything or receive access credentials that do not work.

KIDFLIX: A CSAM STREAMING PLATFORM ON THE DARK WEB

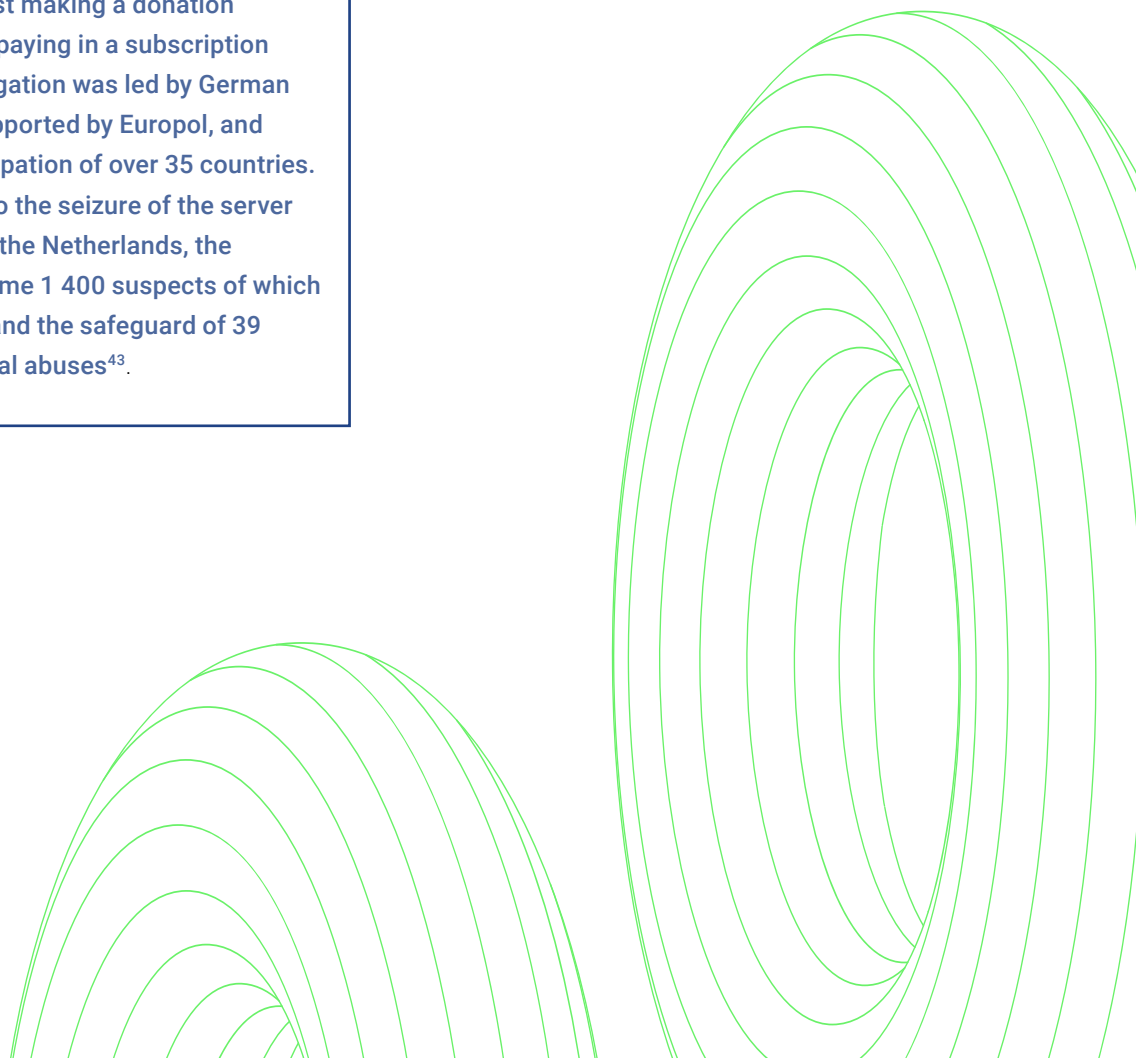
Kidflix was a CSAM streaming platform on the dark web, taken down by LE in 2025. During its activity from 2021 to 2025, the platform had more than 1.8 million users registered and about 80 000 uploaded videos. There were different types of account: basic, premium and admin. With a basic account, users had access only to previews or videos of low quality. Gaining access only required setting up an account with a new username and password. To get full access users needed to obtain a premium account, which could be obtained in exchange for activity on the platform (upload videos, like, rate or comment content). By performing these activities, users would obtain digital coins, called 'candies', and after gaining a certain amount, they would obtain a premium account.

The second possibility was to pay in cryptocurrency, first making a donation and then continue paying in a subscription model. The investigation was led by German authorities and supported by Europol, and involved the participation of over 35 countries. These efforts led to the seizure of the server that was hosted in the Netherlands, the identification of some 1 400 suspects of which 79 were arrested, and the safeguard of 39 children from sexual abuses[43].

Live Distant Child Abuse: a persistent criminal activity in the EU

EU-based consumers mostly purchase live-streamed CSAM of abuses happening in non-EU countries, but cases of CSAM made of victims abused in the EU are also reportedly sold among EU consumers.

The Philippines continues to be a hotspot for LDCA, probably partly influenced by the widespread fluency in English and fast and reliable internet connection in the country. In addition, it is most likely related to established cooperation mechanisms in place and an enhanced national effort in combating CSE. Intelligence suggests that many victims are located in other regions, however these instances remain under-detected. Prices of live-streaming sessions are relatively low, leading to frequent and repeated abuse of victims.



4.3 E2EE applications for networking and exchange of CSAM

An ever-increasing number of group chats dedicated to CSE is hosted on E2EE messaging applications. These applications allow for networking, exchange of CSAM and victims' grooming. A high amount of first-generation CSAM has been identified in investigated groups. E2EE provide high protection from LE scrutiny and given their easy accessibility, they allow for a larger userbase, including offenders who wouldn't have neither the technical capabilities nor will to access the dark web or other environments.

Similar to known patterns in forums in the dark web, these groups operating on E2EE facilitate not only networking and the exchange of CSAM, but also function as 'education' environments, where offenders freely exchange best practices on abuses and countermeasures. In order to avoid LE infiltration, many of these groups have vetting systems for new members who want to join the group. Groups sometimes migrate from one app to another to diversify communication channels, but also if there are suspicions that the hosting application cooperates with the authorities.

THE COM NETWORK AND THE LINKS WITH CSE

Interconnected with the CSE criminal landscape, online communities under the umbrella of **The Com** network pose an extremely serious threat to children and society as a whole. The criminal endeavours carried out by these online communities are multiple, creating a complex landscape where CSE, cyber-attacks, extortion, assault, rape, murder, and violent extremism intertwine. The network is extremely dangerous and combating it is a national priority in several MS and third countries[II].

These networks are largely composed of children, aged between 8 and 17. At the core of their activities lays manipulation and violence, which are a constant feature. There is a full range of individual motivations to join such communities, with some actors engaging in criminal activity for sexual gratification, social reward or a sense of belonging[44]. Some members are driven by a wish to cause fear and chaos, justifying their criminal actions with ideological belief systems. In many cases, the drivers for engagement in the network's criminal activities replicate those that appear in gaming environments.

Offenders often target potential victims on gaming platforms popular among children, and in some cases even on channels used by youth to discuss mental/physical difficulties. Vulnerable children are then groomed on social media and messaging applications with the love-bombing technique. Once sensitive information and compromising images are shared by the victim, the perpetrator uses those to force the child into producing more self-generated sexual material or perform and capture any other violent acts against themselves or others.

The extreme violence, the tremendously high mental and physical health impact on victims, the joining of different criminal activities and actors, and the many investigative challenges linked to data access and E2EE applications, make this online phenomenon particularly threatening. By constantly shifting their activities between different digital spaces and E2EE channels, The Com remains elusive and expands its influence and reach.

[II] For example, in December 2025, Canada formally designated the 764 network (including Maniac Murder Cult and Terrorgram Collective) as a terrorist entity defining it a transnational ideologically motivated violent extremist network. This listing grants law enforcement enhanced powers to counter it. https://www.canada.ca/en/public-safety-canada/news/2025/12/government-of-canada-lists-four-new-terrorist-entities0.html

4.4 Production of synthetic CSAM is on the rise

The rapid evolution of AI tools and the ease of access to them has created more advanced opportunities for offenders, improving the quality of their grooming techniques and scaling up the production of CSAM with the introduction of **AI-generated material.** Investigations on AI-generated material have already emerged, with the identification of platforms made of international communities of offenders dedicated to the production and distribution of synthetic CSAM, where they also exchange of technical skills to improve quality, ready-made prompts, as well as operational security tips.

The accessibility of AI tools has multiplied the volume of CSAM available online, creating additional challenges in the analysis of imagery and identification of offenders. There are two main types of AI-generated CSAM, either fully synthetic or partially synthetic. The latter is usually generated with image-to-image models that are able to modify existing images and produce AI-altered CSAM.

Fully synthetic images are usually generated with text-to-image models, where the user inserts a prompt and obtains the desired image. Text-to-video models have emerged, following the rapid development of text-to-image models. In order to overcome content moderation and obtain accurate results, AI-generated CSAM is often produced in offline models trained with authentic sexual abuse material. Bots editing images to produce synthetic CSAM have also been detected in E2EE groups.

MONTHLY SUBSCRIPTION TO AI-GENERATED CSAM

A subscription business that gave paying customers access to high-quality AI-generated CSAM as well to exclusive communities of AI offenders was created and managed by a 28-year-old suspect, who was also producing AI-generated CSAM and distributing it on the online platform. The exclusive community of AI offenders had around 1 500 members who were exchanging tips on how to best exploit technology to obtain CSAM and how to avoid detection. Customers were from 29 countries worldwide. The platform's administrator was firstly arrested in Denmark in 2024, in an investigation led by Denmark and supported by Europol and the J-CAT, with the involvement of 19 countries. Further coordinated actions in 2025 resulted in the identification of 273 suspects and 25 arrests worldwide[45].

Looking ahead

The cybercrime landscape will continue to present LEAs with an array of evolving challenges, making a proactive and strategic approach more necessary than ever. In the coming years, law enforcement's ability to tackle cybercrime will depend on its capacity to harness innovative technologies, to be able to lawfully access critical data, and to collaborate more closely with the private sector. Below some examples of how the future of cybercrime might look like.

The rise of autonomous cybercrime

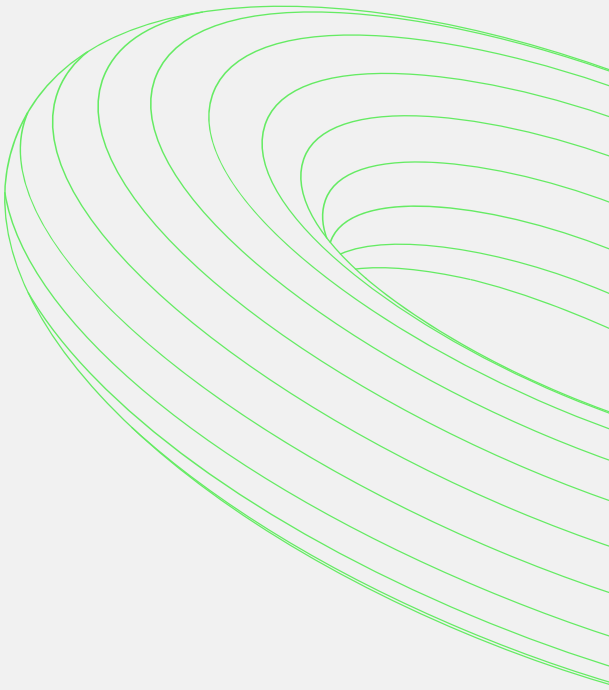
Cybercrime actors have already begun leveraging agentic AI systems capable of autonomously conducting entire criminal workflows with little to no human involvement. As adoption accelerates, these systems will further enable offenders to distance themselves from illicit operations, transforming cybercrime into an increasingly intangible and evasive threat.

Hybrid threats, between ransomware and hacking coalitions

The relationships between state-sponsored hybrid threats and cybercrime actors will continue to pose challenges to society as a whole. DDoS attacks will likely continue to be used as a means to undermine public confidence and trust in governments' ability to protect their citizens and critical infrastructure, instilling insecurity and triggering political instability. The cyber-attacks landscape will likely remain dynamic, with the emergence of hacking coalitions targeting governments, private companies and customers' data, and carrying out cyber-attacks as well as fraud schemes.

More synthetic CSAM and abuse of E2EE

Synthetic CSAM will further expand the variety and severity of child sexual exploitation, exposing victims to deeper and longer-term harms. Social media platforms are likely to remain crucial environments for CSE offenders, and the widespread adoption of E2EE by popular tech companies will continue to thwart swift and effective detection and referral mechanisms. The fight against CSE and online violent extortion networks will be increasingly challenged by the availability of decentralised platforms, which offer high levels of privacy and minimal monitoring.



Online fraud: AI-driven schemes and resilient networks

OFS are expected to continue leveraging AI for various aspects of the criminal process, from sophistication of social engineering to infrastructure management. AI-driven fraud will mean simultaneous multi-tasking, and replacing labour-intensive operations with autonomous digital workforce. On the other hand, the resilience of online fraud networks - especially those relying on CaaS - is based on their ability to legally purchase and activate SIM cards in bulk. As long as bulk purchasing and registration protocols are possible, networks will be able to regenerate their infrastructure indefinitely. Countering the use of SIM boxes requires robust anti-spoofing measures and enhanced identity verification processes in the telecommunications industry.

Cybercrime and financial enablers

Cybercriminals' use of exchange services in non-EU jurisdictions with loose anti-money laundering (AML) standards continues to create barriers to international cooperation. A fragmented regulatory landscape for cryptocurrency oversight impedes authorities' coordination across borders, resulting in enforcement gaps and reduced accountability. In addition, the integration of neo-banks into criminal operations reflects the evolution of criminals' fintech abuse. Strengthening LEAs power of action against services that are non-compliant with current EU AML regulations is therefore paramount.

Appendix

METHODOLOGY

The Internet Organised Crime Threat Assessment (IOCTA) is a strategic analysis report providing an assessment of the latest threats and the impact of cybercrime to the EU. The report provides a law enforcement centric view of the threats and developments related to cybercrime, in order to inform decision-makers at strategic, policy and tactical levels in the fight against cybercrime, and with a view to updating the operational focus for EU law enforcement authorities.

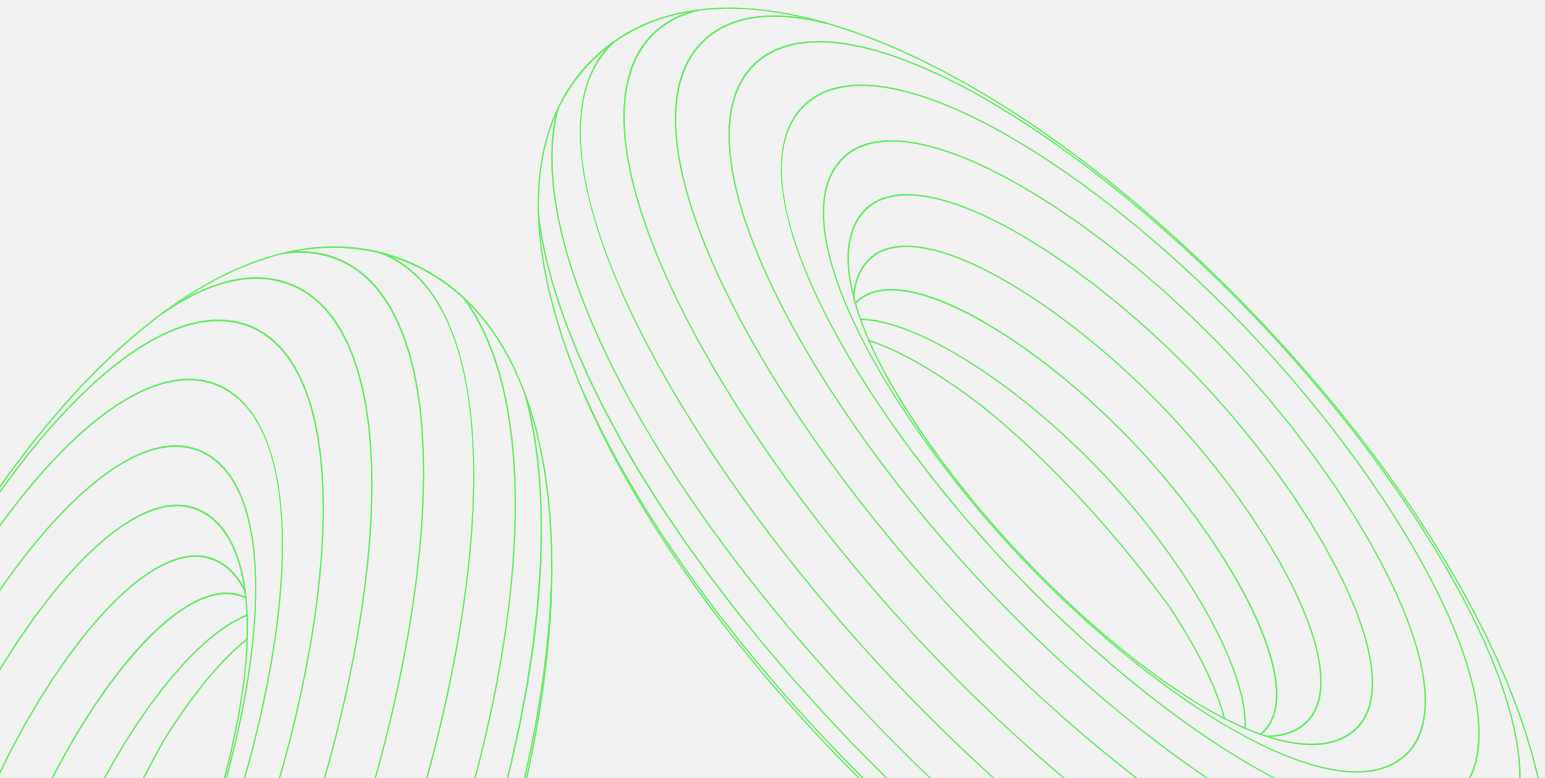
Europol's first threat assessment on Internet Facilitated Organised Crime was published in 2011. Since then, the threat assessment is a regular product issued on a yearly basis.

The assessment of the threat is based on a set of indicators established by Europol, focusing on developments related to criminal actors and networks, criminal processes, infrastructure used, financial transactions, and the impact on society.

SOURCES

Criminal intelligence stemming from operational activities supported by Europol's European Cybercrime Centre (EC3) constitutes the core dataset for the analysis. EU Member States and operational cooperation partners contribute this information to Europol, which is continuously monitored, thoroughly analysed and enriched by additional sources. The criminal intelligence is related to major investigations supported by Europol in 2025.

Additionally, the assessment draws on the knowledge and expertise of subject matter experts from EC3. The collected data consists primarily of qualitative information complemented by internal and external reports and open-source information.



Abbreviations

2FA Two-factor Authentication

2G Second Generation

AI Artificial Intelligence

AML Anti-Money Laundering

AMM Automated Market Makers

AP Analysis Project

ATO Account Takeover

BEC Business Email Compromise

C2 Control-and-Command

CaaS Crime-as-a-service

CEO Chief Executive Officer

CSAM Child Sexual Abuse Material

CSE Child Sexual Exploitation

CSP Communication Service Provider

DDoS Distributed Denial of Service

DeFI Decentralised Finance

DEX Decentralised Exchange

DNS Domain Name System

E2EE End-to-End Encryption

EC3 European Cybercrime Centre

ENISA European Union Agency for Cybersecurity

EU European Union

EUR Euro

IAB Initial Access Broker

ID Identity Document

IMSI International Mobile Subscriber Identity

IP Internet Protocol

J-CAT Joint Cybercrime Action Taskforce

KYC Know Your Customer

LDCA Live-Distance Child Abuse

LE Law Enforcement

LEA Law Enforcement Agency

LLM Large Language Model

ML Money Laundering

MS Member State

NATO North Atlantic Treaty Organization

NCMEC National Center for Missing & Exploited Children

NFT Non-Fungible Tokens

OFS Online Fraud Scheme

OTP One-Time Password

RaaS Ransomware-as-a-service

RDP Remote Desktop Protocol

SIM Subscriber Identity Module

SMS Short Message Service

SOC Serious and Organised Crime

SSL Secure Socket Layer

TOR The Onion Router

USD United States Dollar

USDT United States Dollar Tether

VLOP Very Large Online Platform

VDS Virtual Desktop Service

VPN Virtual Private Network

References

1 Europol, 2025, Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

2 Europol, 16 June 2025, Europe-wide takedown hits longest-standing dark web drug market, accessibile at https://www.europol.europa.eu/media-press/newsroom/news/europe-wide-takedown-hits-longest-standing-dark-web-drug-market

3 Europol, 20 January 2025, Law enforcement takes down two largest cybercrime forums in the world, accessible at https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-takes-down-two-largest-cybercrime-forums-in-world

4 ICANN, November 2025, DNS Abuse Mitigation Program, accessible at: https://www.icann.org/dnsabuse

5 Europol, 1 December 2025, Europol and partners shut down cryptomixer. accessible at: https://www.europol.europa.eu/media-press/newsroom/news/europol-and-partners-shut-down-cryptomixer

6 Unit 42, 25 November 2025, The Dual-Use Dilemma of AI: Malicious LLMs, accessible at https://unit42.paloaltonetworks.com/dilemma-of-ai-malicious-llms/

7 Europol, 2025, European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

8 Digital Service Act, 2025, Very large online platforms and search engines, accessible at: https://digital-strategy.ec.europa.eu/en/policies/dsa-vlops

9 Europol 2025, 17 October 2025, Cybercrime-as-a-service takedown: 7 arrested, accessible at https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

10 European Association for Secure Transactions (EAST), 2025, European Payment Terminal Crime Report, accessible at https://www.association-secure-transactions.eu/intranet/crime-reports/

11 European Association for Secure Transactions (EAST), 2025, Security Update: Data relay attack, accessible at https://www.association-secure-transactions.eu/wp-content/uploads/secure/EAST-EGAF-and-EPTF-Security-Update-2026-001-Data-Relay-Attack.pdf

12 Binance, 2004, Angel Drainer Absorbs Inferno's Toolkit, Becoming a Larger Threat to Crypto Wallets, accessible at https://www.binance.com/en/square/post/15096207996425

13 Europol, 27 October 2025, Position Paper on Caller ID Spoofing, accessible at https://www.europol.europa.eu/publications-events/publications/position-paper-caller-id-spoofing

14 Europol, 17 October 2025, Cybercrime-as-a-service takedown: 7 arrested, accessible at https://www.europol.europa.eu/media-press/newsroom/news/cybercrime-service-takedown-7-arrested

15 European Commission, 2025, eIDAS Regulation, accessible at https://digital-strategy.ec.europa.eu/en/policies/eidas-regulation; European Commission, 2025, Implementing and delegated acts - PSD 2, accessible at https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/payment-services-directive_en

16 _Europol, 2025, European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

17 Europol, 2025, Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

18 Checkpoint, 2025, The State of Ransomware – Q2 2025, accessible at https://research.checkpoint.com/2025/the-state-of-ransomware-q2-2025/

19 CISA, Cybersecurity Advisory, #StopRansomware: Akira Ransomware, accessible at https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a

20 Europol, 20 February 2024, Law enforcement disrupt world's biggest ransomware operation, accessible at https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation

21 Bleeping Computer, 7 May 2025, LockBit ransomware gang hacked, victim negotiations exposed, accessible at https://www.bleepingcomputer.com/news/security/lockbit-ransomware-gang-hacked-victim-negotiations-exposed/

22 Trend Micro, 25 September 2025, New LockBit 5.0 Targets Windows, Linux, ESXi, accessible at https://www.trendmicro.com/tr_tr/research/25/i/lockbit-5-targets-windows-linux-esxi.html

23 Trend Micro, 29 October 2025, Ransomware Spotlight DragonForce, accessible at https://www.trendmicro.com/vinfo/us/security/news/ransomware-spotlight/ransomware-spotlight-dragonforcel

24 Europol, 11 February 2025, Key figures behind Phobos and 8Base ransomware arrested in international cybercrime crackdown, accessible at https://www.europol.europa.eu/media-press/newsroom/news/key-figures-behind-phobos-and-8base-ransomware-arrested-in-international-cybercrime-crackdown

25 Intel471, 28 February 2025, Black Basta exposed: A look at a cybcercrime data leak, accessible at https://www.intel471.com/blog/black-basta-exposed-a-look-at-a-cybercrime-data-leak

26 Bleeping Computer, 7 April 2025, Everest ransomware's dark web leak site defaced, now offline, accessible at https://www.bleepingcomputer.com/news/security/everest-ransomwares-dark-web-leak-site-defaced-now-offline/ ; Bleeping Computer, 20 February 2025, Black Basta ransomware gang's internal chat logs leak online, accessible at https://www.bleepingcomputer.com/news/security/black-basta-ransomware-gang-s-internal-chat-logs-leak-online/

27 Ibid

28 CISA, 4 June 2025, Cybersecurity Advisory, #StopRansomware: Play Ransomware, accessible at https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-352a

29 Krebs on Security, 02 February 2026, Please Don't Feed the Scattered Lapsus ShinyHunters, accessible at https://krebsonsecurity.com/2026/02/please-dont-feed-the-scattered-lapsus-shiny-hunters/

30 Krebs on Security, 24 September 2025, Feds Tie 'Scattered Spider' Duo to $115M in Ransoms, accessible at https://krebsonsecurity.com/2025/09/feds-tie-scattered-spider-duo-to-115m-in-ransoms/

31 Krebs on Security, 24 September 2025, Feds Tie 'Scattered Spider' Duo to $115M in Ransoms, accessible at https://krebsonsecurity.com/2025/09/feds-tie-scattered-spider-duo-to-115m-in-ransoms/

32 MSSP Alert, 22 April 2022, Lapsus$ Cyberattack Victim List: Globant, Microsoft, Nvidia, Okta, Samsung, T-Mobile, accessible at https://www.msspalert.com/news/alleged-lapsus-cyberattack-victim-list-grows-microsoft-nvidia-okta-samsung-more

33 Picus Security, 20 October 2025, Scattered LAPSUS$ Hunters: 2025's Most Dangerous Cybercrime Supergroup, accessible at https://www.picussecurity.com/resource/blog/scattered-lapsus-hunters-2025s-most-dangerous-cybercrime-supergroup ; Krebs on Security, 7 October 2025, ShinyHunters Wage Broad Corporate Extortion Spree, accessible at https://krebsonsecurity.com/2025/10/shinyhunters-wage-broad-corporate-extortion-spree/

34 Europol, 2025, Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/Steal-deal-repeat-IOCTA_2025.pdf

35 Europol, 2025, Press Release https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-follow-leads-to-five-detentions-and-interrogations-well-server-takedowns

36 Europol, 2025, Operation ENDGAME strikes again: the ransomware kill chain broken at its source, accessible at https://www.europol.europa.eu/media-press/newsroom/news/operation-endgame-strikes-again-ransomware-kill-chain-broken-its-source

37 Europol, 13 November 2025, End of the game for cybercrime infrastructure: 1025 servers taken down, accessible at https://www.europol.europa.eu/media-press/newsroom/news/end-of-game-for-cybercrime-infrastructure-1025-servers-taken-down

38 Europol, 2025, European Union Serious and Organised Crime Threat Assessment - The changing DNA of serious and organised crime, Publications Office of the European Union, Luxembourg, accessible at https://www.europol.europa.eu/cms/sites/default/files/documents/EU-SOCTA-2025.pdf

39 Cloudflare, 15 July 2025, Hyper-volumetric DDoS attacks skyrocket: Cloudflare's 2025 Q2 DDoS threat report, accessible at https://blog.cloudflare.com/ddos-threat-report-for-2025-q2/

40 Europol, 16 July 2025, Global operation targets NoName057(16) pro-Russian cybercrime network, accessible at https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network?utm

41 National Center for Missing & Exploited Children (NCMEC), 2025, Spike in online crimes against children a "wake-up call", accessible at https://www.missingkids.org/blog/2025/spike-in-online-crimes-against-children-a-wake-up-call

42 Europol, 2025, Help4U: A lifeline for young people facing online sexual abuse, accessible at https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/help4u-lifeline-for-young-people-facing-online-sexual-abuse

43 Europol, 2025, Global crackdown on Kidflix, a major child sexual exploitation platform with almost two million users, accessible at https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-kidflix-major-child-sexual-exploitation-platform-almost-two-million-users

44 FBI, 2025, Public Service Announcement, Violent Online Networks Target Vulnerable and Underage Populations Across the United States and Around the Globe, accessible at https://www.ic3.gov/PSA/2025/PSA250306

45 Europol, 2025, 25 arrested in global hit against AI-generated child sexual abuse material, accessible at https://www.europol.europa.eu/media-press/newsroom/news/25-arrested-in-global-hit-against-ai-generated-child-sexual-abuse-material

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

www.europol.europa.eu