EUROPOL

IOCTA

Internet Organised Crime Threat Assessment

2025

Steal, deal and repeat

How cybercriminals trade and exploit your data

Steal, deal and repeat - How cybercriminals trade and exploit your data
Internet Organised Crime Threat Assessment (IOCTA) 2025

PDF WEB

ISBN 978-92-9414-027-2 ISSN 2363-1627 doi: 10.2813/4926508 QL-01-25-009-EN-N

Luxembourg: Publications Office of the European Union, 2025

Cite this publication: Europol, *Steal, deal and repeat - How cybercriminals trade and exploit your data – Internet Organised Crime Threat Assessment*, Publications Office of the European Union, Luxembourg, 2025.

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

Contents

Key findings

- Data theft is a significant threat. Compromised data is being highly valuable to a wide range of criminal actors who exploit it as a commodity in its own right, but also as a target to be acquired for other purposes, including the perpetration of further criminal activities.

- Cybercriminals use a variety of techniques to access and steal personal data, exploiting both system vulnerabilities and human oversight. These techniques are employed by various criminal actors who often combine them at the different stages of the criminal process. Social engineering stands out as a particularly prevalent technique.

- The wider adoption of Large Language Models (LLMs) and other forms of generative artificial intelligence are improving the efficacy of social engineering techniques by tailoring communication with the victims and automating criminal processes.

- A thriving part of the criminal ecosystem revolves around selling access to compromised systems and accounts. Initial Access Brokers (IABs) are increasingly advertising these services, along with related commodities, on specialised criminal platforms used by a wide range of cybercriminals.

- Data brokers are spreading their activities across multiple platforms in order to diversify their operations and increase their resilience against law enforcement operations. End-to-end encrypted (E2EE) communication apps are increasingly being used to negotiate and conduct sales transactions involving breached data, as well as to share the personal information of targeted victims, including children.


IOCTA
IOCTA
IOCT
IOCT
IOC
2025

Introduction

Serious and organised crime is evolving at an unprecedented pace as it adapts to a world in flux with alarming speed and agility. As crime becomes more sophisticated, it is progressively destabilising our society, with illicit activities increasingly being nurtured online. Artificial Intelligence (AI) and other cutting-edge technologies are accelerating the dark side of the digital revolution, with cybercriminals exploiting them to increase the scale and efficiency of their operations[1].

The online domain has become an integral and ubiquitous part of daily life. Today, a wide variety of criminal activities take place primarily or entirely online, with digital infrastructure and the data it holds becoming prime targets for criminals.

Data has become a key commodity, serving both as a target and a key enabler in the cybercrime threat landscape[2]. Its value lies in its ability to facilitate a wide range of criminal activities, including cyber-attacks, online fraud schemes, sexual exploitation of children online, and extortion. Consequently, demand for data is skyrocketing and its illicit trade is expected to become even more widespread in underground economies, contributing to the destabilisation of legitimate economies and the erosion of trust in governance structures. The theft and compromise of personal data can have severe consequences, undermining the functioning of society and having a serious impact on those affected.

The illicit data ecosystem can also be exploited by Advanced Persistent Threat (APT)[A] and other types of hybrid threat actors[B] who can collaborate with criminal networks and leverage their resources to further their agendas. By infiltrating secure systems, they can steal data of strategic importance for governments or businesses and provide hybrid threat actors with invaluable information that can then be used for espionage, economic advantage or even coercion[3]. Furthermore, hybrid threat actors may exploit stolen data and access services to launch cyber-attacks against governments and critical infrastructure, resulting in widespread disruption and instability [C].

The emerging use of (AI) in criminal business models has added a new layer of complexity to the threat landscape. Cybercriminals may use AI for attack automation, social engineering and bypassing security measures, enabling more scalable and complex attacks. AI-driven techniques may facilitate data acquisition, while the data itself can also be weaponised in AI-enabled attacks — for instance, to generate deepfakes, synthetic media and false identities.

In light of these findings, and given the identification of trade in stolen data as a key threat — particularly in relation to the crime-as-a-service (CaaS) market — this edition of the IOCTA takes a deep-dive into unauthorised access, data brokers, and data markets. The report provides a comprehensive analysis of how cybercriminals trade and exploit illegal access to data and how they commodify these goods and services, while also examining the complex criminal ecosystem that surrounds them.

A **Advanced persistent threat (APT) groups** are threat actors often sponsored and/or operated by nation states. APT actors are well-resourced and engage in sophisticated malicious cyber activity, which objectives could include espionage, data theft, network/system disruption or destruction.

B **Hybrid threat** actors can be state or non-state actors seeking to undermine a target, such as a state or institution, through a (combination of) a variety of means to fulfil their strategic objectives. [Hybrid CoE, Hybrid threats as a concept, accessible at https://www.hybridcoe.fi/hybrid-threats-as-a-phenomenon/]

C Considering Europol's current mandate, this report will focus on exploring the exploitation of data and access from a (cyber)criminal perspective.

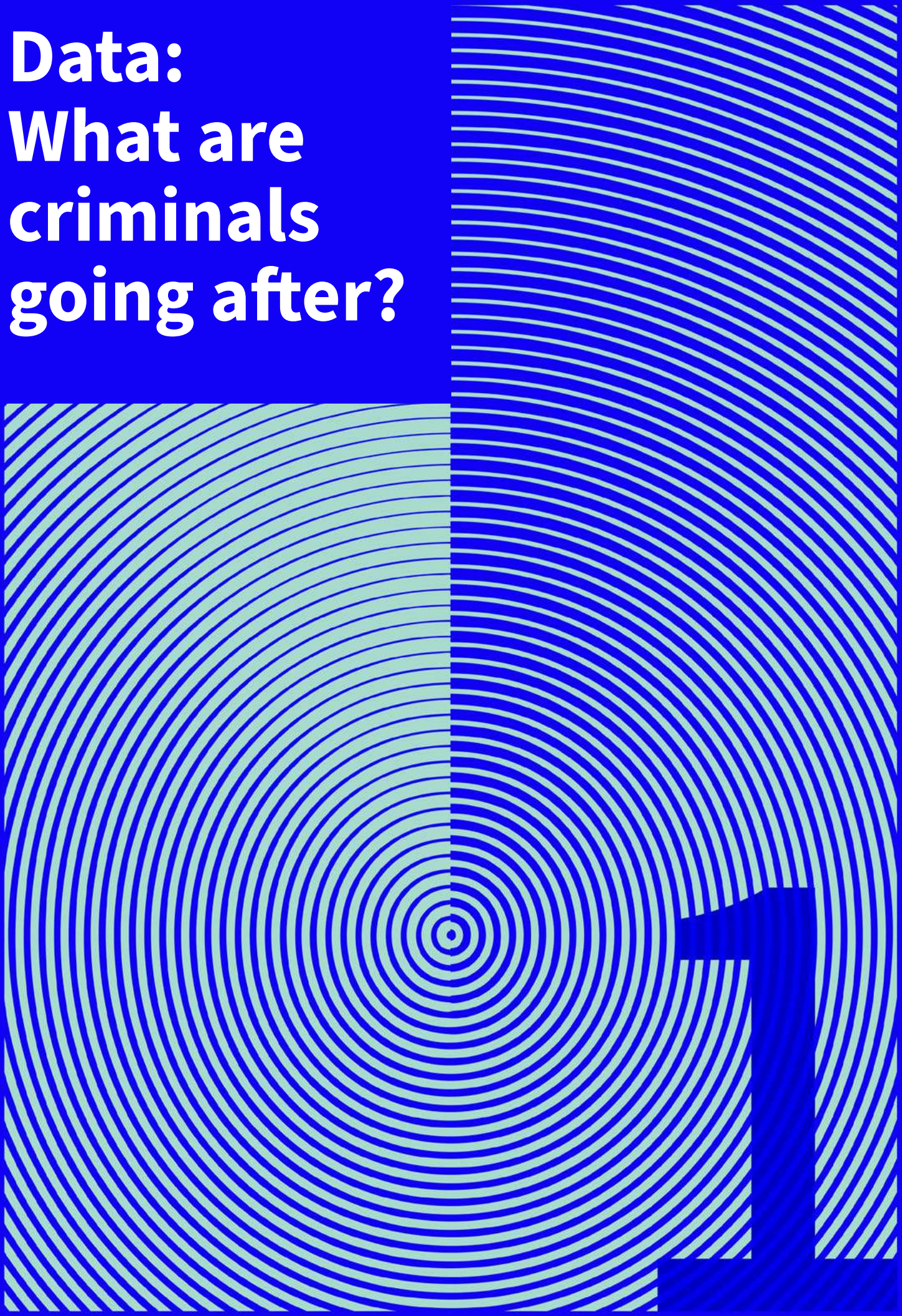
Methodology

Data for this year's IOCTA has been collected from a variety of sources. These include an analysis of cases supported by the Europol European Cyber Crime Centre (EC3), interviews with Europol operational team experts, and input from members of Europol EC3 Advisory Groups[4].

The report is also informed by other Europol intelligence analysis products, in particular the EU Serious and Organised Crime Threat Assessment (EU-SOCTA) 2025. Where relevant, open-source information has been used as a complementary data source.

Europol experts and Advisory Groups have provided specialised insights into the different types of data commodities, how they are acquired and exploited, profiles of initial access and data brokers, and the functioning of criminal platforms dedicated to data trade. However, as many of these transactions take place in closed communication channels, it should be noted that this report only covers the parts of the ecosystem that are visible to EC3.

Data: What are criminals going after?



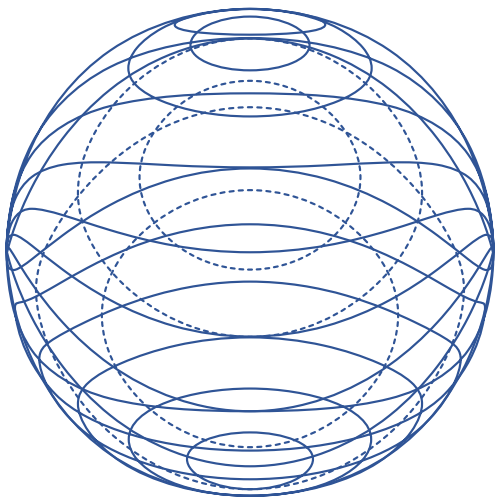
Data is the central commodity of the cybercrime economy — sought after, stolen, bought and exploited by a wide range of offenders[5]. It is relevant to a variety of criminal processes and belongs to individuals and private and public entities alike.

The rapid digitalisation of everyday life, including retail, public services, financial services, social interactions, and communication, has resulted in an ever-growing volume of information being held in digital systems and openly online. This information is vulnerable to exploitation. In addition, the increased complexity of most digital infrastructure, combined with the speed of transition and insufficient digital literacy among users, leaves more systems vulnerable to cyber-attacks targeting this data[6].

Data, in the broad sense, refers to any type of information, from access credentials to remote services, accounts and personal information[D]. Access credentials to remote services and interfaces, such as Remote Desktop Protocols (RDPs), Virtual Private Networks (VPNs) and cloud environments, can give criminals access to networks.

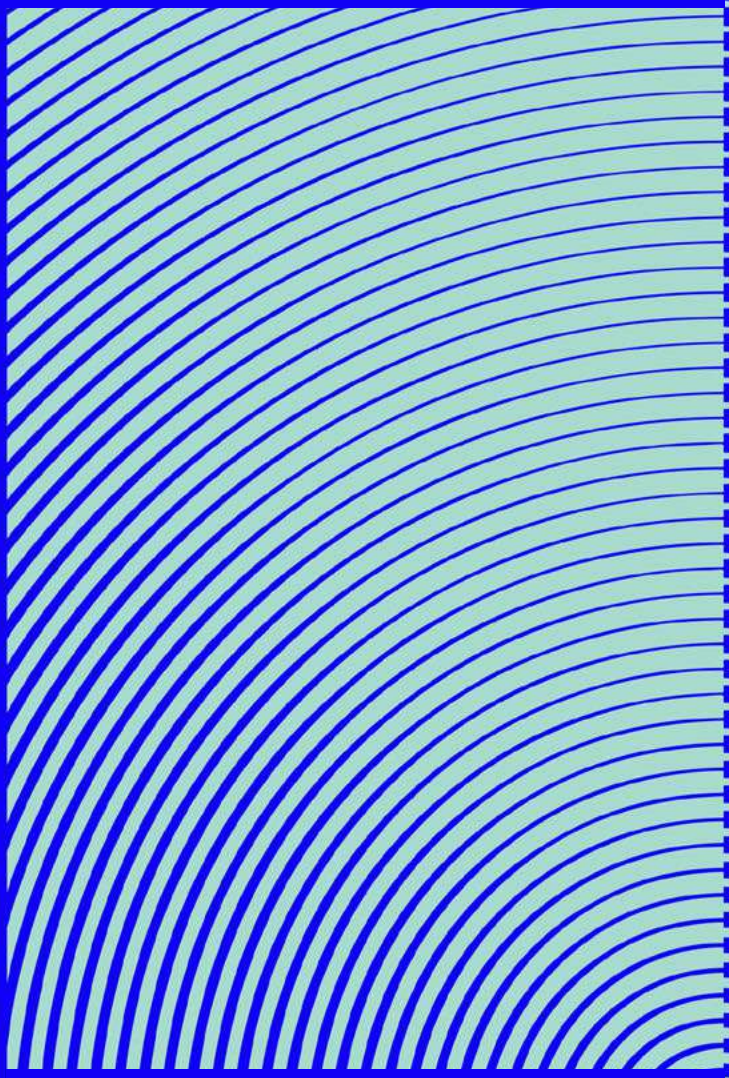
Access credentials to personal accounts are also valuable assets because they provide direct access to mailboxes, social media accounts, online shops, financial services and public administration information systems where additional sensitive information is stored. A wide range of valuable personal information is also shared openly by individuals, especially on social media platforms. This can lead to a person being identified and relevant links to their private life being found, including contacts, location, family and work relations.

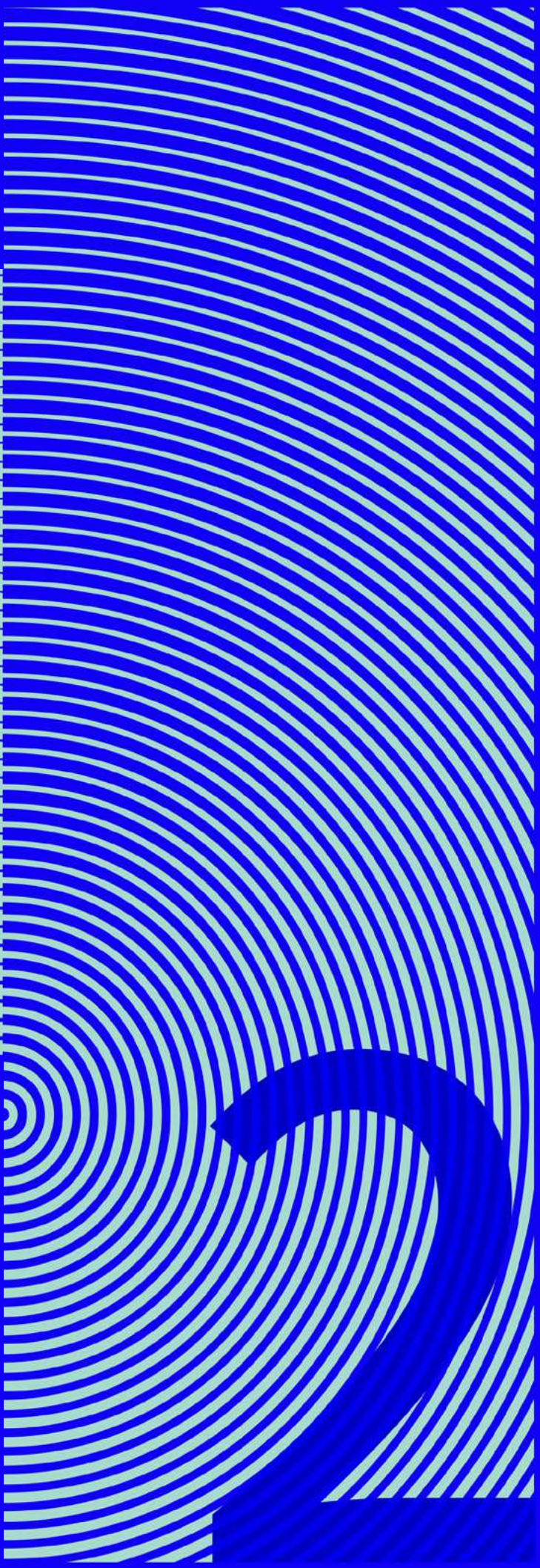
Access to a victim's account or system is the critical part of most cybercrime kill chains, as it can be used to compromise the wider network (lateral movement), distribute malware, steal sensitive information, impersonate the victim and/or use the account to distribute malicious content from a trusted source[7]. These breaches usually lead to further data in the victim's account, device or system being compromised, effectively creating a vicious cycle that fuels cybercrime.



D Personal data, also known as personal identifiable information (PII), is any information that relates to an identified or identifiable living individual (data subject). Different pieces of information, which together can lead to the identification of a particular person, may also be considered personal data. [Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, accessible at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e1489-1-1].

How is data exploited?





All this data is interconnected and, in many cases, co-dependent, strongly linked to access to systems and to more data. This makes it valuable to criminal actors who are aware of these co-dependencies and exploit it as a final commodity, a target to be acquired for other purposes and a means to perpetrate further criminal activities. Depending on the intended criminal activity, different types of data are exploited through a variety of specific techniques.

2.1 Data as a target

Most cyber-attacks have data as their main target, as it is highly valuable to its owners. Cybercriminals use different methods to access and acquire said data. These methods can serve several criminal processes in which information can be used as a leverage for monetary demands, either by taking it hostage, encrypting it or by threatening to release it (ransomware). Cybercriminals can use access credentials for email, social media and financial services for various cyber-attacks, online fraud schemes and to steal funds, as well as to gain unauthorised access to digital assets and sensitive information[8].

Other actors, driven by commercial or geopolitical interests, may target information for espionage purposes. This data often belongs to businesses and public entities and its loss can disrupt services and cause monetary loss and reputational damage. This type of data often includes sensitive information about clients, users and other third parties.

2.2 Data as a means

Personal data is particularly valuable to the perpetrators of crimes such as fraud and child sexual exploitation (CSE) as preparatory means of achieving their criminal goals. Criminals involved in online fraud schemes use various types of personal information to profile their targets, increasing the success of their fraud, or to gain unauthorised access to victim's accounts. This includes details such as an individual's age, interests and location. These enable criminals to create more credible and manipulative fraud narratives around their victims. It also includes email addresses, dates of birth, phone numbers and credit card data. When combined, these details can be used to access the targets' monetary funds.

Both fraud and CSE perpetrators collect personal information to tailor their communication with the victims and use it as leverage for sexual and financial extortion. The data includes the victims' interests, their personal connections, home and school addresses, as well as information about their close relatives and friends. Collecting this information can also be used for doxxing — the act of publicly exposing and shaming victims by publishing their private information online. This can also lead to other offenders targeting the same victim, and to cyber-bullying and re-victimisation of children.

Identity theft remains a major concern. Criminals use stolen personal data to create fake identities, apply for subsidies, loans or credit cards and commit other types of financial fraud. For example, in Business Email Compromise (BEC) attacks, criminals impersonate company executives or employees to trick others into transferring funds or revealing sensitive information.

2.3 Data as a commodity

Information is stolen and converted into a commodity to be further exploited by other criminal actors in their operations. It is then marketed on various criminal platforms, including specialised marketplaces, underground forums, and dedicated channels within end-to-end encrypted (E2EE) communication apps. Listings and offers vary according to the type of data and the intended buyer. They include sensitive data, business information, credit card details and web service access credentials. This data can be used for credential stuffing — the use by criminals of automated tools to try stolen login credentials on multiple websites and applications.

How are data and access acquired?

Cybercriminals use a variety of techniques to access personal data that exploit either system vulnerabilities or human oversight. These techniques cater to different criminal actors who often combine them at the different stages of the criminal process.

3.1 Exploiting human vulnerabilities: social engineering techniques

Social engineering, which exploits human error to gain access to systems or personal information, stands out as a prominent technique used by criminal actors in this context. Initial Access Brokers (IABs) have been increasingly focused on using such techniques for the acquisition of valid account credentials as an entry point to the victims' systems. This initial access can then be leveraged in a multitude of ways by criminal actors. For example, access credentials for remote services are widely used by ransomware groups and their affiliates to compromise corporate networks, which can lead to data theft (exfiltration) and the deployment of ransomware[9].

Valid account credentials can be obtained using several **phishing** techniques. The most well-known approaches involve infecting victims with malware or tricking them into entering their credentials on fraudulent websites created using phishing-kits[10]. These kits are widely available in the CaaS economy and enable criminals to purchase imitations of legitimate websites for the purpose of stealing login credentials.

Malware commonly deployed for data theft includes **infostealers**, a category of malware specifically designed to illicitly extract sensitive information from compromised devices. Infostealers are used to both steal login credentials and collect application tokens and session cookies, which can then be used to access to websites and applications as an authenticated user[11]. In addition, they collect information about the user's device, operating system and settings, as well as browser data. This information can then be used to imitate the target's digital fingerprint[E]. This enables criminals to bypass some security features during account takeovers, because they can configure the fingerprint of their virtual machine to mimic that of the legitimate user.

TAKEDOWN OF INFOSTEALER INFRASTRUCTURE

In 2025, Europol partnered up with Microsoft and supported the second part of the international law enforcement operation **Endgame**, targeting the complex ecosystem that allowed criminals to exploit stolen information on a massive scale. Lumma, the world's largest infostealer, was a sophisticated tool that enabled cybercriminals to collect sensitive data from compromised devices on a massive scale. Stolen credentials, financial data, and personal information were harvested and sold through a dedicated marketplace, making Lumma a central tool for identity theft and fraud worldwide.

The Lumma marketplace operated as a hub for buying and selling the malware, providing criminals with user-friendly access to advanced data-stealing capabilities. Its widespread use and accessibility made it a preferred choice for cybercriminals looking to exploit personal and financial data. Microsoft identified over 394 000 Windows computers globally infected by the Lumma malware.

Phishing techniques are the main vector for the distribution of infostealers[F]. Criminals use a variety of methods to achieve this, including sending emails, text messages or messages on social media that contain malicious attachments or URLs which introduce malware into the victim's system. Malicious websites are also propagated through search engine advertising tools and search engine optimisation (SEO) poisoning. In the latter case, criminals manipulate web search results to lead users to websites containing malware.

E **Digital fingerprint** is a user-specific set of attributes related to browsing and digital behaviour, which can be used to confirm their identity when logging into their accounts.
F **Infostealers** are malicious software designed to gather information from the infected system.

These websites can masquerade as legitimate sites for downloading popular software or content, or they can be compromised sites that display content or contain scripts that execute upon visit. Infostealers can also be distributed through malicious applications and browser extensions that are available in legitimate app stores[12].

In addition, a technique commonly referred to as ClickFix is becoming increasingly popular among cybercriminals. Users may encounter dialogue boxes containing fake error or CAPTCHA messages while browsing the internet. These messages trick users into copying, pasting and running malicious content on their own computer. Pop-ups usually display a dialogue box that require the user to press buttons labelled 'Fix It' or 'I am not a robot'. Once clicked, either a malicious PowerShell script is copied into the PowerShell terminal or Windows Run dialogue box or users receive instructions on how to manually execute the malware[13].

Vishing, the use of fraudulent phone calls tricking victims into providing sensitive information, is enabled by the prevalence of spoofing services[G], which allow criminals to impersonate local and reputable entities that suit the needs of their narrative, increasing the effectiveness of social engineering. The technique is widely used to perpetrate frauds and to gain initial access to systems. Vishing, which is becoming increasingly popular, involves the persuasion of victims to download malicious payloads, enter their credentials on phishing websites, or install legitimate Remote Access Tools (RATs) or Remote Monitoring and Management (RMM) tools on their devices[14]. This is a well-known approach used by fraudsters who impersonate customer support employees of an IT solution providers to gain access to victims' bank accounts. It appears that IABs and ransomware operators are now increasingly adopting this approach to harvest valid VPN and user account credentials[15].

While there are many ways in which criminals can access victims' systems and data from the outside, there are also several ways in which threat actors can do the same from the inside. Insider threats can be created by either recruiting an employee to exfiltrate information or install backdoors on corporate networks, purchasing valid login credentials from current or former staff members or through impersonation.

The latter refers to the creation of fake online profiles that enable threat actors to apply for jobs in companies and leverage their position to compromise corporate systems from within[16].

The efficacy of many of the aforementioned social engineering techniques has been improved by the wider adoption of LLMs and other forms of generative artificial intelligence (genAI). Phishing texts and scripts, generated to incorporate the language and cultural nuances of the victims' location, can improve the efficacy of campaigns[17]. Recent research on the topic indicates that phishing messages generated by LLMs have a significantly higher click-through rate than those likely written by humans[18]. CSE perpetrators use LLMs to tailor their communication, creating highly personalised and convincing messages and easily impersonating peers to obtain personal information for further exploitation. This can make it harder for victims to recognise the manipulation, as communication may seem more genuine and tailored to their specific interests and circumstances. The automation of this process by LLMs enables CSE offenders to scale up their online grooming operations, targeting multiple victims in several languages simultaneously and making their exploitation efforts more efficient[19]. Criminals can also use voice deepfakes to increase the credibility of spear-phishing campaigns used for BEC and CEO fraud[20]. As discussed above, genAI can also be exploited to generate fake social media profiles using a range of social engineering applications.

G A service that allows users to make phone calls with fake or constantly changing phone numbers or send emails appearing them to originate from a reputable source.

3.2 **Exploiting system vulnerabilities**

Techniques that exploit vulnerabilities in the targeted systems are often used in combination with, or as an alternative to, social engineering. IABs continue to keenly monitor and exploit vulnerabilities in organisations' public facing infrastructure (e.g. web servers, network devices, firewalls, VPNs and other cloud infrastructure). Cybercriminals also continue to target the webpages and apps of online retail platforms with digital skimming[H] attacks in order to steal credit card details and/or account login credentials.

Common Vulnerability Exposures (CVEs) enable a range of attack vectors, which allow criminals to gain access to systems and/or collect valid account credentials and digital payment data. For example, software vulnerabilities can enable remote code execution, allowing criminals to run malicious code on a device or within a network. They can also carry out replay attacks[I] to retrieve transmitted data. Cybercriminals may also position themselves within a communication channel between networked devices in order to manipulate or intercept transmitted data. This process is often referred to as Man-in-the-Middle (MitM) attack.

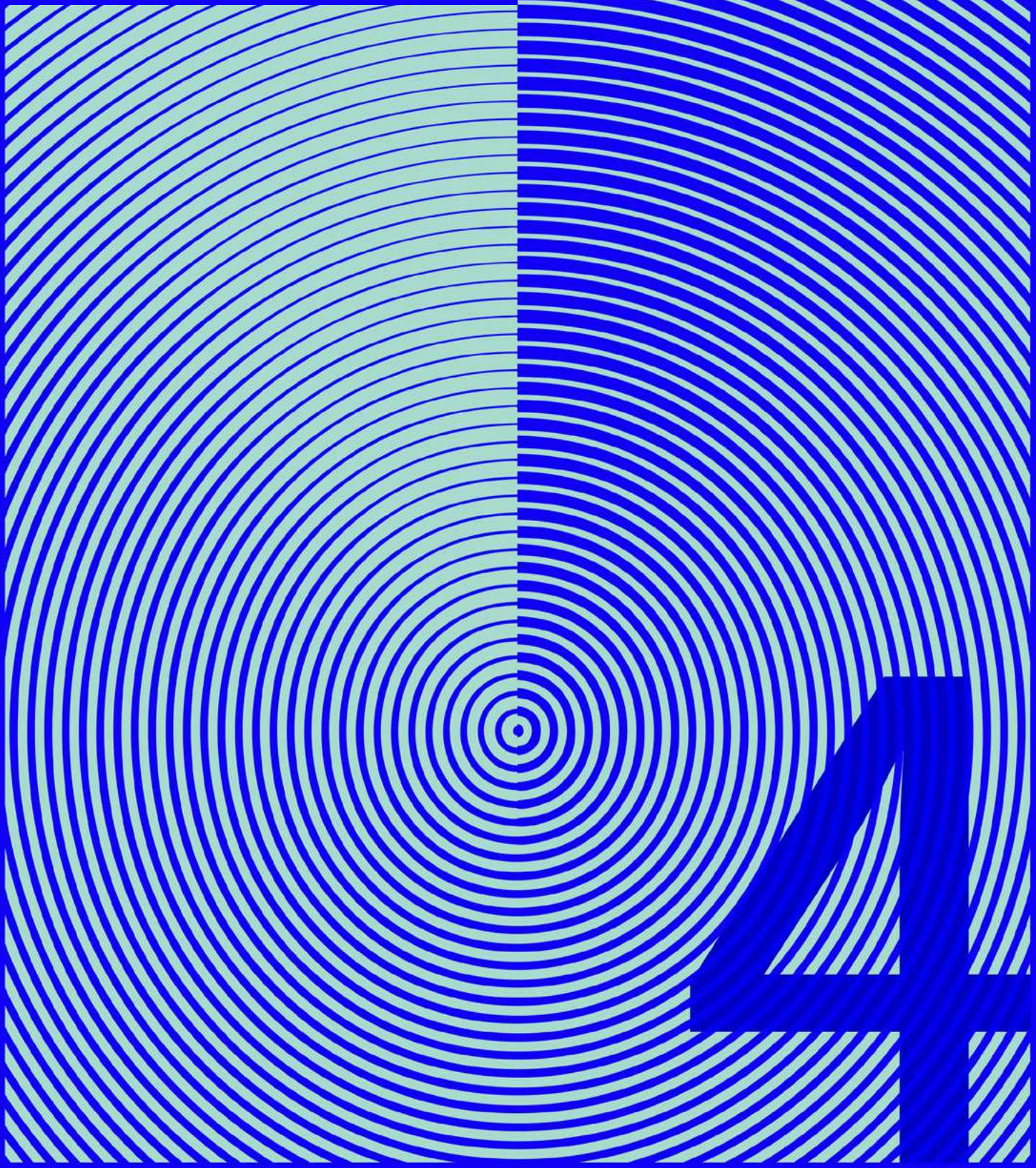
Brute force attacks can be used for automated password guessing to acquire valid account credentials. For example, this can be done using previously acquired or leaked data sets. It can also be done offline to crack the password hashes captured through MitM attacks. Similarly, criminals can exploit the publicly available Bank Identification Numbers (BINs) on payment cards to generate valid card numbers for fraudulent use (BIN attacks)[21].

Criminals can also forge user credentials for web apps and services using session cookies, tokens and other artefacts to authorise user access. Web apps and services often use session cookies as an authentication token once a user has logged in to a website. These cookies are often valid for an extended period of time, even if the web app is not actively used[22].

H A **web skimmer** is a JavaScript code injected by an attacker onto a website with the specific intent of stealing any kind of sensitive data willingly entered by the user, such as credit card details or passwords.

I A **replay attack** involves the interception of secure network communication that is then fraudulently resent or delayed, maintaining its original characteristics, avoiding detection and making it appear legitimate to the receiver.

Who are the criminal actors?

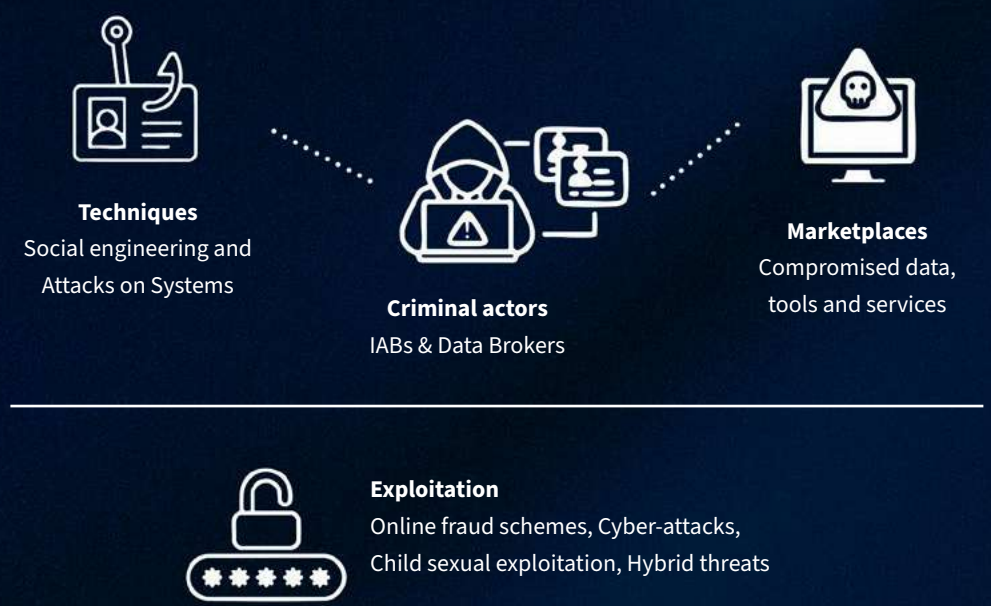


Cybercriminals who specialise in data theft and initial access brokering deploy a wide range of methods in their operations. They adapt their criminal processes to the target, making it difficult to create clear-cut profiles. They target victims and systems *en masse* and try to capitalise on exposed technical and human weaknesses. This opportunistic approach is also reflected in the broad range of tools and techniques they use, which are chosen based on suitability and availability.

For example, data and login credential brokers use infostealers, which are offered as-a-service on criminal platforms, to gather information from their victims. They also use botnet-based dropper services to orchestrate phishing and malspam campaigns and malvertising services, as well as other techniques, to distribute malware. The stolen data, such as infostealer logs and breached data dumps, can be sold or further processed by criminals to extract credentials and other information. It is likely that there are criminals who specialise in extracting and analysing this type of information and offer their services to those running and using infostealer services.

DISRUPTING THE MALWARE DISTRIBUTION ECOSYSTEM

In 2024, Europol supported two international law enforcement operations, called **Endgame**[23] and **Magnus**[24], which disrupted the malware distribution ecosystem by taking down some of the most prominent dropper[J] and infostealer services widely used by cybercriminals. The infostealers taken down, RedLine and META, targeted millions of victims worldwide, making them one of the largest malware platforms globally. The droppers, which were offered as-a-service, included IcedID, SystemBC, Pikabot, Smokeloader, Bumblebee and Trickbot, used their network of infected computers (a botnet) to deliver malware (e.g. an infostealer) to victims' systems via malspam campaigns. Following these large-scale operations, cybercriminals have started to diversify their techniques in order to compensate for the loss of these popular malware services.



J **Droppers** are programs designed to deliver malicious software to a device. They usually do not have malicious functions themselves and are designed to evade and de-activate the system's security features (e.g. anti-virus (AV), endpoint detection) before installing malware and other malicious tools (i.e., payloads).

IABs also utilise exploit kits to compromise systems with unpatched known vulnerabilities, and brute force attacks to access misconfigured services. Stolen valid user credentials, combined with other intrusion techniques enable them to establish persistence in a compromised system, which they then sell on cybercriminal platforms.

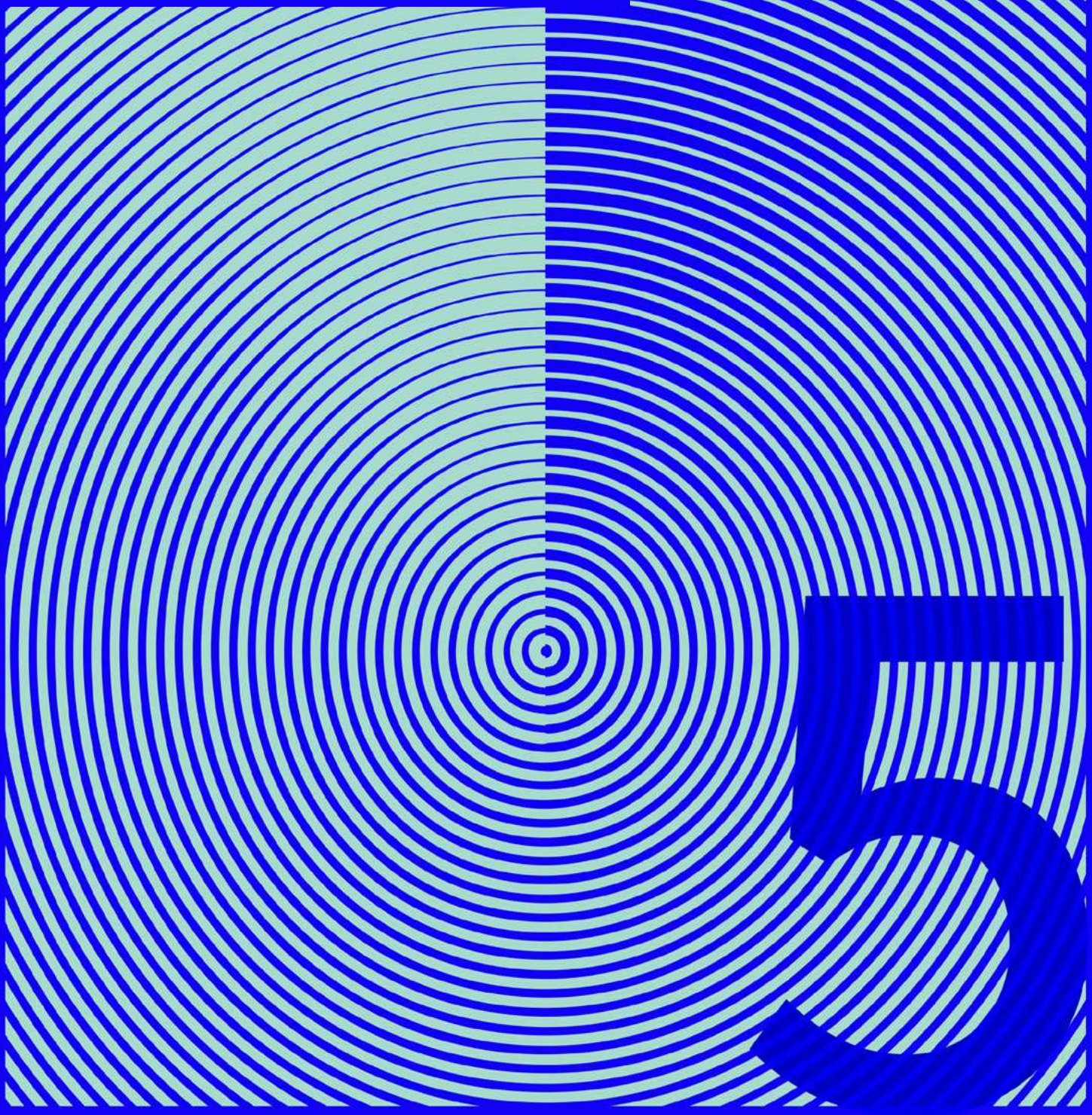
Advanced IABs and hybrid threat actors (e.g. APTs) use the methods mentioned above but also more sophisticated techniques that enable them to compromise valuable targets such as digital service providers (supply-chain attacks), international corporations and government entities. This includes finding and creating zero-day exploits[K], as well as carrying out complex, targeted social engineering operations. These types of actors usually do not advertise their capabilities on public platforms but rather monetise their exploits by collaborating directly with cybercrime groups (e.g. ransomware groups) or hybrid threat actors[25]. This means that valuable assets, like zero-day exploits and access to valuable targets, such as large international corporations, IT supply chains and critical infrastructure, are traded privately, possibly in exchange for a percentage of the buyer's earnings.

The criminal actors who target financial data and access to payment systems are the main customers of criminal services that offer phishing-kits and digital skimmers. The URLs of the created fraudulent webpages are disseminated through phishing campaigns and web-skimmers inserted into misconfigured or unpatched websites. These techniques are similar to ones used by data and access brokers. Stolen account information or payment card details are often sold via dedicated online platforms specialising in the respective commodities.

The final category of actors includes CSE and certain fraud perpetrators, such as those involved in romance fraud, who do not seek to commodify the personal data they gather from their victims but rather exploit it as an essential part of their criminal processes. Instead of trading in data, they use it directly to access accounts or coerce their victims. However, not all CSE offenders act alone. Doxxing channels on E2EE applications have been identified, demonstrating a collective effort to amplify their coercive power[26]. In these environments, criminal actors cooperate by sharing the personal data they have gathered on their targets, magnifying the pressure imposed on the victims who are subjected to multiple, simultaneous extortion processes.

K A zero-day is a vulnerability or security hole in a computer system unknown to its owners, developers or anyone capable of mitigating it. Until the vulnerability is patched, threat actors can exploit it via what is called a zero-day exploit.

Where are data and access commodified?



Cybercriminals can purchase the different types of data they exploit, as well as the tools and services used to acquire it, through a variety of cybercriminal platforms, predominantly hosted on the dark web.

These commodities[L] include:

- Unanalysed infostealer logs and breached data dumps (leaked or stolen data), which may contain personal data, user credentials for various services, browser artefacts[M] and other sensitive information;
- Unanalysed or verified credit card dumps (usually gathered by digital skimming), as well as the bulk sale of verified card details;
- Initial access offers, ranging from credentials for remote services and accounts (e.g. RDP, VPN, firewalls, network devices and cloud environments) to established backdoor access to corporate systems and networks;
- Account login credentials for various web services, including email and social media accounts, online shopping environments and adult content sites;
- Criminal services, including subscriptions to phishing-kits, infostealers, exploit kits, droppers, spoofing services and malicious LLMs;
- Anti-detection solutions, such as VPNs, bulletproof hosting (BPH), residential proxies[N], money laundering services, operational security (OpSec) manuals, etc.[27]

These commodities can be advertised and sold on platforms such as cybercriminal markets and/or forums. Some marketplaces and forums specialise in particular types of commodities (e.g. compromised credit card data), while others offer information and services relating to various cybercrime domains. Larger, more generalised forums are increasingly giving way to smaller, more specialised channels that cater to specific areas of cybercrime[28]. In addition, criminals are increasingly using E2EE channels as an extension of these platforms, where they advertise, sell and purchase goods and services.

5.1 Fraud-related data

Dark web platforms cater to a broader range of cybercriminals. The commonly traded commodities that are most often used to facilitate fraud include compromised credit card data and account login credentials for web services (e.g. streaming, online shopping environments and adult content sites)[29].

Automated vending carts (AVCs) are marketplaces specifically used for the sale of compromised card details. These automated websites allow buyers to search through listings based on various factors and purchase items without interacting with a vendor. Data sets are typically advertised using samples, with the full set becoming available upon purchase. Carding[O] marketplaces also offer card-testing services for criminals who have harvested or purchased unverified dumps of credit card information.

Manuals, guidelines and tutorials, as well as individual coaching sessions, are widely available. These are often related to OpSec and explain how to carry out online fraud schemes. Such products are often inexpensive and are sometimes included as an add-on with the sale of another product or service[30].

Anti-detection solutions such as VPNs, BPH and money laundering services, as well as subscription-based access to phishing and exploit kits and infostealers, are also readily available. BPH providers are increasingly leveraging networks of residential proxies that function as perpetual botnets, because they are always active, very rarely patched and usually not protected by security software. Providers of infostealer CaaS are also expanding the functionalities of their malware. For example, they are turning the infected devices into residential proxies as an additional monetisation strategy[31].

L In this context, commodity refers to any digital asset, resource, or service that can be readily bought, sold, or traded within the cybercriminal ecosystem.
M For example, bookmarks, navigation history, downloaded file lists, cache data.
N Residential proxies refer to compromised home appliances, network devices (e.g., routers) and other endpoints with residential IPs.
O Fraudulent use of verified stolen credit card details, frequently to purchase prepaid cards. Lists of verified card details may also be resold for other criminals to use.

HALTING THE TRADE OF PHISHING-KITS

In 2024, Europol supported an international operation that severely disrupted LabHost[32], a major platform that offered phishing-kits for sale. Accessible via the clear net, the marketplace offered customisable phishing kits, hosting infrastructure, interactive functionality for engaging with victims directly, as well as campaign overview services for a monthly subscription fee of around USD 250. Law enforcement authorities uncovered at least 40 000 phishing domains linked to LabHost, which had around 10 000 users worldwide.

5.2 Initial access (Access brokers)

A thriving part of the criminal ecosystem involves selling access to compromised systems and accounts. According to CrowdStrike, IAB activity surged in 2024, with the price of advertised access increasing by almost 50 %[33].

Some platforms, such as the Russian Market[34], specialise in selling stolen identities, access credentials, web shells[P] and financial information. Access credentials, for example, can be sold in bulk, meaning that their validity and value has not been verified. Validated credentials and other listings posted by IABs, advertising the systems to which they have access, are usually accompanied by the details of the compromised entities and sometimes auctioned to the highest bidder.

Data may be sold and purchased several times by different criminal actors, or resold after use. This can result in multiple actors launching attacks against the same victim[35].

The prices charged depend on the commodities and can vary significantly based on the compromised entity's sector, size, revenue, geographical location, access type, level, and persistence, and the exclusivity of the offer. High-revenue companies in Europe and North America are in high demand.

These specialised platforms are popular with lower-level affiliates of ransomware groups, who use these commodities as initial access points in their attacks.

5.3 Breached data (data brokers)

Forums dedicated to breached data, such as BreachForums[36], are used as advertising spaces, while the negotiations and transactions between the customers and vendors increasingly take place on dedicated channels on commercial E2EE communication platforms[37]. The listings do not only advertise available commodities but are also used to build the seller's reputation within the ecosystem. Compromising more prominent and valuable targets enhances standing in the community [38]. For this reason, many data brokers also overstate the classification or value of their assets whereas in reality their offerings may be fake or related to outdated leaks, which they advertise to attract attention[39].

Groups specialising in infostealer logs often redirect to their channels on E2EE apps, which interested parties can request to join. Approval by a channel administrator may be required in order to join, and invitation links often expire after a certain amount of time. Various subscription structures and prices may apply, ranging from weekly to annual and from tens to hundreds of USD. Access to more exclusive products may be conditional upon the party attaining a higher membership status[40].

P **A web shell** is a script that is used to interact with and maintain access to a system after an initial compromise.

Data brokers who operate across multiple platforms diversify their operations and increase their resilience against law enforcement actions. If a forum is seized, they do not need to rebuild their reputation from scratch, but can simply continue to advertise their dedicated channels on a different platform.

5.4 **Culture**

Criminals gather in forums, seeking to connect with like-minded individuals and discuss ways to develop their skills. Criminal networks, based on these interactions, also use these environments for the recruitment of individuals with specific skill sets for their operations. Data brokers and IABs use these forums as advertising platforms for their products and services.

Participation in criminal marketplaces and forums is based on trust and an individual's reputation within the underground community. Building an online reputation is essential for full engagement, including viewing restricted posts and access to all content. In some cases, a deposit may be required before newcomers can view any listings[41]. For sellers of products and services, a good reputation and the implied trust that this engenders will ensure sales. A good reputation is often necessary for buyers to access valuable listings, such as corporate systems, as these would become invalid if they fell into the hands of law enforcement[42]. A solid reputation may also be valuable in case of dispute resolution.

A good reputation is built on factors such as a long-term stable presence on forums and marketplaces, quantity of posts, successful deals, positive reviews and endorsement by other reputable community members[43].

To emphasise their trustworthiness, criminals also seek to establish themselves in moderator positions or obtain badges to enhance their sense of personal achievement and belonging. A good reputation is especially important for people in roles related to forum management, as it helps them maintain their customer base across the criminal markets in which they operate. Users with a long-standing and proven reputation are more trusted and preferred as business partners. If their user base is reputable and considered more highly skilled, the reputation and prominence of forums themselves will be greater[44].

CYBERCRIME FORUMS DISMANTLED

Up until their recent takedown by international law enforcement[45] in January 2025, the cybercrime forums Cracked and Nulled were among the largest in the world. They were key marketplaces for stolen data, including personal data, and cybercrime tools and infrastructure, which were offered as-a-service to individuals with more limited technical skills to carry out cyber-attacks. The two forums also offered AI-based tools and scripts that could automatically scan for security vulnerabilities and optimise attacks. Cracked had over four million users and listed more than 28 million posts advertising cybercrime tools and stolen information, generating approximately USD 4 million in revenue. One product advertised on Cracked offered users access to 'billions of leaked websites', allowing them to search for stolen login credentials.

With more than five million users and over 43 million posts advertising cybercrime tools and stolen information, Nulled generated approximately USD 1 million in revenue per year[46].

Discussion

Open society

The digital manifestation of the concept of an 'open society', characterised by vast amounts of easily accessible personal data fuelled by both voluntary online sharing and pervasive commercial data brokering, presents unique paradoxes. While this environment fosters connectivity, its inherent transparency also creates significant vulnerabilities.

It can heighten risks for the most vulnerable, particularly children, as offenders exploit easily accessible personal details to identify and groom their victims. Data often innocently shared by children or their guardians, such as names, locations, images and interests, can be meticulously gathered by offenders and used to create profiles, groom and ultimately exploit minors. At the same time, the general abundance of available data dramatically simplifies intelligence gathering for criminal and hybrid threat actors who seek to harm the broader population.

Access to data

Conversely, criminals are increasingly exploiting E2EE apps to impede investigations. Technically, E2EE blocks service providers from accessing communication content, rendering warrants for lawful access unserviceable within the EU. This creates a lack of visibility of, and ability to investigate, criminal activity.

When content is blocked by E2EE, metadata becomes essential for mapping networks and identifying suspects. However, the current legislative landscape lacks harmonised rules and this results in fragmented national policies. Consequently, crucial metadata, such as subscriber information or IP logs, is often subject to short or inconsistent retention periods. This means that it is frequently deleted before complex investigations, particularly cross-border ones, have an opportunity to secure it.

Abuse of AI

The increasing use of AI models by criminals adds another layer of complexity. For example, AI can be used to commit sophisticated crimes involving the abuse of biometric data through harvested digital photos and deepfake technology for impersonation. AI can also be used by employing adversarial learning to create fake digital fingerprints capable of bypassing security measures such as two-factor authentication (2FA). These methods demonstrate that criminals are actively leveraging the imperfections and capabilities of AI to innovate attack vectors and evade detection[47].

At the same time, new tactics such as slopsquatting[48] exploit AI code assistant errors to inject malware into software supply chains. These assistants sometimes suggest non-existent software libraries or packages[49]. Malicious actors monitor these AI suggestions. Once they have identified a package that has been 'hallucinated' repeatedly, they create a real but malicious package with the same name and upload it to public repositories. If developers trust the AI's suggestion and use the code without verifying the existence of the package, their systems may automatically download and install the attacker's malicious package, resulting in a software supply chain attack.

Dispersion of intelligence, crime and punishment

The evolving technological landscape has also resulted in intelligence and law enforcement-like actions dispersing beyond State control. While hacktivist data leaks potentially offer intelligence on adversaries, they create challenges in terms of validation, admissibility, and investigation interference. Online doxxing further complicates matters by bypassing legal due process and potentially contaminating evidence.

This forces cybercrime investigators to navigate an increasingly complex environment in which diverse criminal and hybrid actors influence the information landscape.

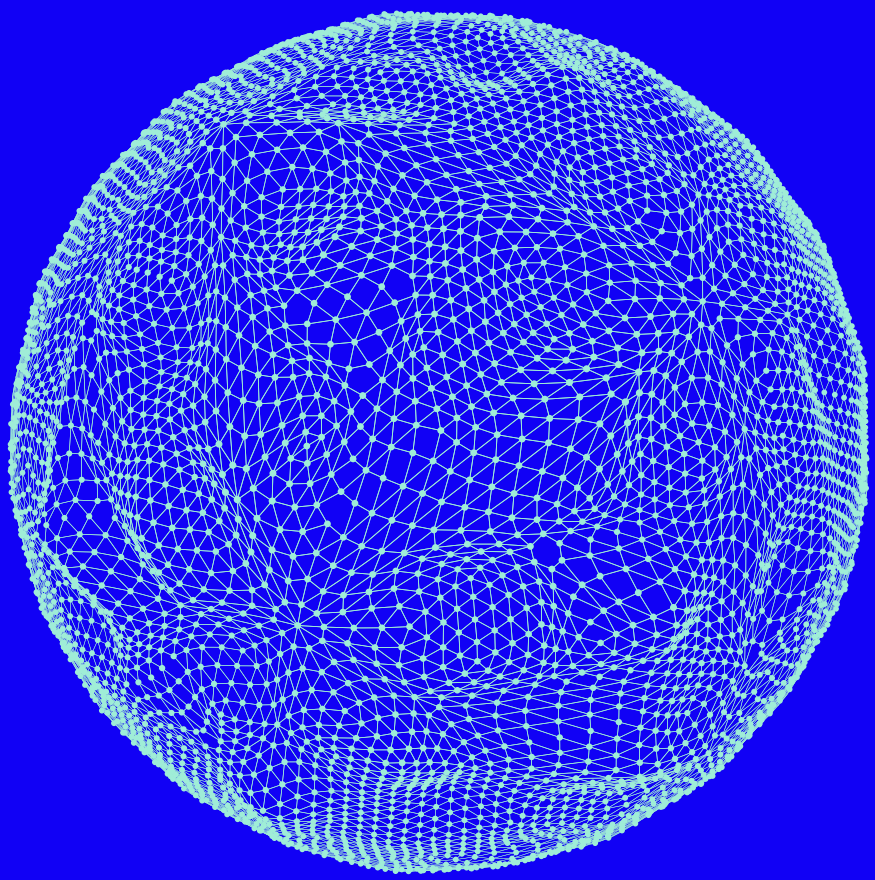
Conclusions

Overcoming the complex challenges outlined above requires multifaceted policy considerations that focus on both societal resilience and enabling effective law enforcement within the EU's robust legal framework. Key actions should include:

Establishing lawful access by design to E2EE communication channels in cooperation with service providers and regulators.

Establishing clear and harmonised EU standards for the targeted retention and/or expedited access to essential metadata, operating strictly within the boundaries defined by CJEU case law (targeting serious crimes and ensuring compliance with the principles of necessity and proportionality), to provide greater legal certainty and improve the effectiveness of cross-border investigations.

Promoting broad digital literacy, critical verification skills and responsible online sharing practices. This should include an emphasis on specific guidance for parents, guardians and young people on online risks and effective privacy management in order to mitigate vulnerabilities stemming from data openness.



Endnotes

1 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

2 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

3 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

4 More information on the Europol EC3 Advisory Groups and their members can be found here: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3/ec3-partners.

5 Europol, 2023, Internet Organised Crime Threat Assessment (IOCTA) 2023, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023.

6 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

7 IOCTA 2023, Cyber-Attacks: The Apex of Crime-as-a-Service, Europol spotlight report, accessible at: https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023.

8 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

9 Europol, 2024, Internet Organised Crime Threat Assessment (IOCTA) 2024, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 ; Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

10 Europol, 2024, Internet Organised Crime Threat Assessment (IOCTA) 2024, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024 ; Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

11 Europol, 2024, Internet Organised Crime Threat Assessment (IOCTA) 2024, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

12 Europol, 2023, Internet Organised Crime Threat Assessment (IOCTA) 2023, Spotlight Report - Cyber-Attacks: The Apex of Crime-as-a-Service, accessible at: https://www.europol.europa.eu/publication-events/main-reports/cyber-attacks-apex-of-crime-service-iocta-2023.

13 ProofPoint, 2024, Security Brief: ClickFix Social Engineering Technique Floods Threat Landscape, accessible at https://www.proofpoint.com/us/blog/threat-insight/security-brief-clickfix-social-engineering-technique-floods-threat-landscape; Group-IB, 2025, ClickFix: The Social Engineering Technique Hackers Use to Manipulate Victims, accessible at https://www.group-ib.com/blog/clickfix-the-social-engineering-technique-hackers-use-to-manipulate-victims/.

14 CrowdStrike, 2025, Global Threat Report, accessible at https://www.crowdstrike.com/en-us/global-threat-report/.

15 Contribution of the EC3 Advisory Group on Internet Security.

16 CrowdStrike, 2025, Global Threat Report, accessible at https://www.crowdstrike.com/en-us/global-threat-report/.

17 TrendMicro, 2025, The Ever-Evolving Threat of the Russian-Speaking Cybercriminal Underground, accessible at https://www.trendmicro.com/vinfo/nl/security/news/cybercrime-and-digital-threats/the-ever-evolving-threat-of-the-russian-speaking-cybercriminal-underground.

18 An academic study on phishing email click-through rates revealed that while rates for human-drafted messages are about 12 %, LLM-generated messages rates are about 54 %. F. Heiding, S. Lermen, A. Kao, B. Schneier, A. Vishwanath, 2024, Evaluating Large Language Models' Capability to Launch Fully Automated Spear Phishing Campaigns: Validated on Human Subjects, accessible at: https://www.researchgate.net/publication/386374220.

19 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

20 Europol, 2023, Internet Organised Crime Threat Assessment (IOCTA) 2023, Spotlight Report - Online Fraud Schemes: A Web of Deceit, accessible at https://www.europol.europa.eu/publication-events/main-reports/spotlight-report-online-fraud-iocta-2023; Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

21 Cybereason, Cracking the Code: How to Identify, Mitigate, and Prevent BIN Attacks, accessible at https://www.cybereason.com/blog/identifying-and-preventing-bin-attacks.

22 Mitre, Steal Web Session Cookie, access at https://attack.mitre.org/techniques/T1539/.

23 Europol, 2024, Largest ever operation against botnets hits dropper malware ecosystem, accessible at https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem.

24 Operation Magnus, https://www.operation-magnus.com/.

25 Europol information; Europol, 2023, Internet Organised Crime Threat Assessment (IOCTA) 2023, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2023.

26 Europol information.

27 Europol, 2024, Internet Organised Crime Threat Assessment (IOCTA) 2024, accessible at https://www.europol.europa.eu/publication-events/main-reports/internet-organised-crime-threat-assessment-iocta-2024.

28 Europol information.

29 Europol information.

30 Europol information.

31 Europol information.

32 Europol, 2024, International investigation disrupts phishing-as-a-service platform LabHost, accessible at https://www.europol.europa.eu/media-press/newsroom/news/international-investigation-disrupts-phishing-service-platform-labhost.

33 CrowdStrike, 2025, Global Threat Report, accessible at https://www.crowdstrike.com/en-us/global-threat-report/.

34 Flare, 2023, Top 5 Dark Web Marketplaces to Monitor, accessible at https://flare.io/learn/resources/blog/dark-web-marketplaces/.

35 Europol, 2025, European Union Serious and Organised Crime Threat Assessment (EU SOCTA) - The changing DNA of serious and organised crime, accessible at https://www.europol.europa.eu/publication-events/main-reports/changing-dna-of-serious-and-organised-crime.

36 Bleeping Computer, 2024, FBI seize BreachForums hacking forum used to leak stolen data, accessible at https://www.bleepingcomputer.com/news/security/fbi-seize-breachforums-hacking-forum-used-to-leak-stolen-data/.

37 Europol information.

38 Contribution of the EC3 Advisory Group on Internet Security

39 Europol information.

40 Europol information.

41 Flare, 2023, Top 5 Dark Web Marketplaces to Monitor, accessible at https://flare.io/learn/resources/blog/dark-web-marketplaces/.

42 TrendMicro, 2025, The Ever-Evolving Threat of the Russian-Speaking Cybercriminal Underground, accessible at https://www.trendmicro.com/vinfo/nl/security/news/cybercrime-and-digital-threats/the-ever-evolving-threat-of-the-russian-speaking-cybercriminal-underground.

43 TrendMicro, 2025, The Ever-Evolving Threat of the Russian-Speaking Cybercriminal Underground, accessible at https://www.trendmicro.com/vinfo/nl/security/news/cybercrime-and-digital-threats/the-ever-evolving-threat-of-the-russian-speaking-cybercriminal-underground.

44 Europol information.

45 Europol, 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.

46 U.S. Department of Justice, 2025, Cracked and Nulled Marketplaces Disrupted in International Cyber Operation, accessible at https://www.justice.gov/opa/pr/cracked-and-nulled-marketplaces-disrupted-international-cyber-operation.

47 TrendMicro, 2025, The Ever-Evolving Threat of the Russian-Speaking Cybercriminal Underground, accessible at https://www.trendmicro.com/vinfo/nl/security/news/cybercrime-and-digital-threats/the-ever-evolving-threat-of-the-russian-speaking-cybercriminal-underground.

48 Bleeping Computer, 2025, AI-hallucinated code dependencies become new supply chain risk, accessible at https://www.bleepingcomputer.com/news/security/ai-hallucinated-code-dependencies-become-new-supply-chain-risk/.

49 J. Spracklen, et al., 2024, We Have a Package for You! A Comprehensive Analysis of Package Hallucinations by Code Generating LLMs, accessible at https://www.researchgate.net/publication/381484725_We_Have_a_Package_for_You_A_Comprehensive_Analysis_of_Package_Hallucinations_by_Code_Generating_LLMs.

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

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

www.europol.europa.eu