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.

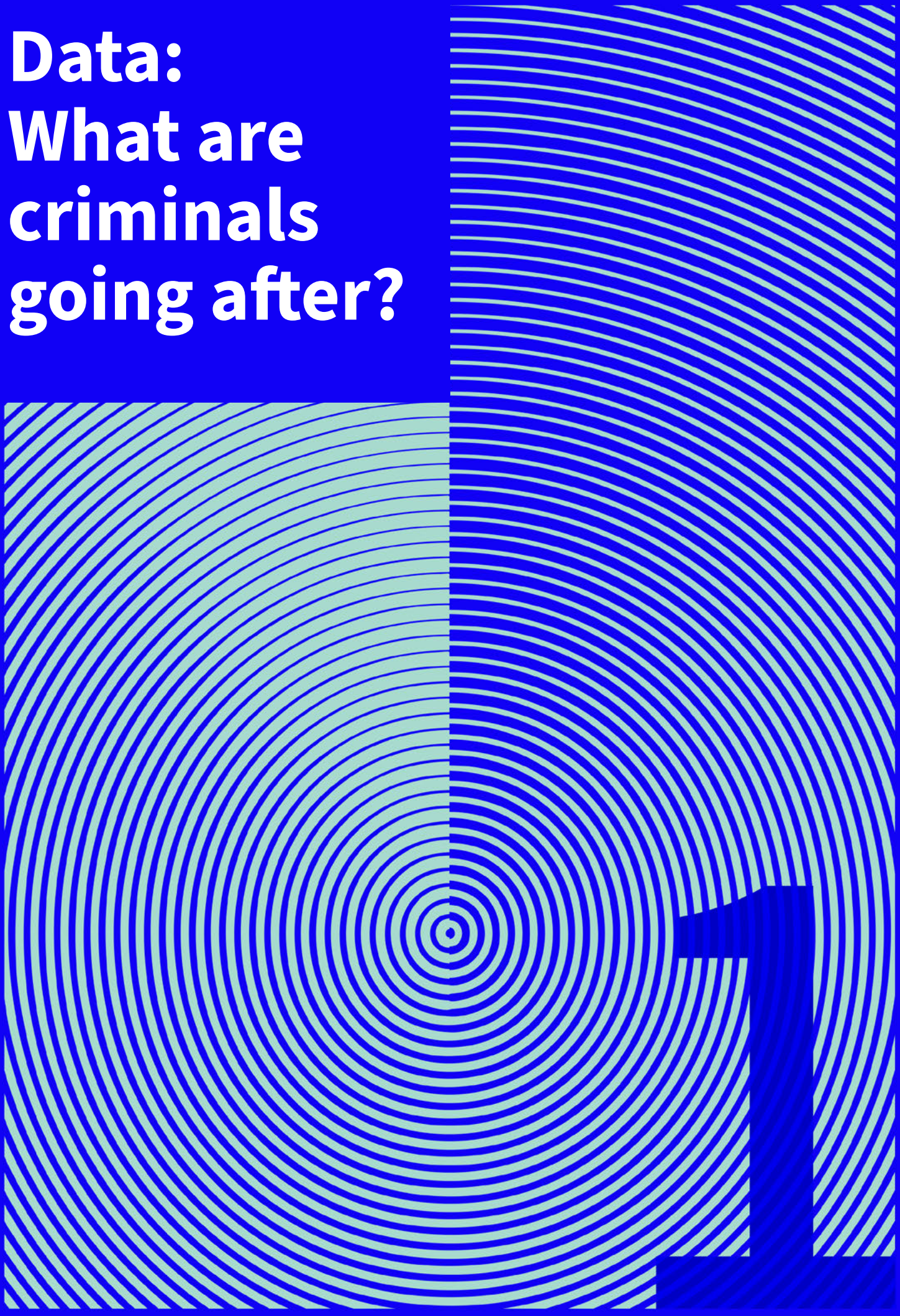
Methodology

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?



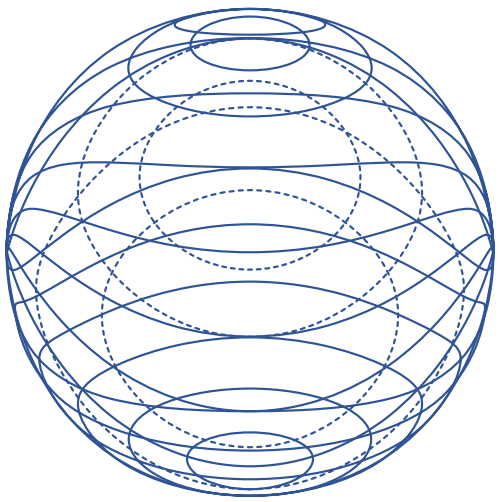
Data is the central commodity of the cybercrime economy — sought after, stolen, bought and exploited by a wide range of offenders[5]. It is relevant to a variety of criminal processes and belongs to individuals and private and public entities alike.

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.

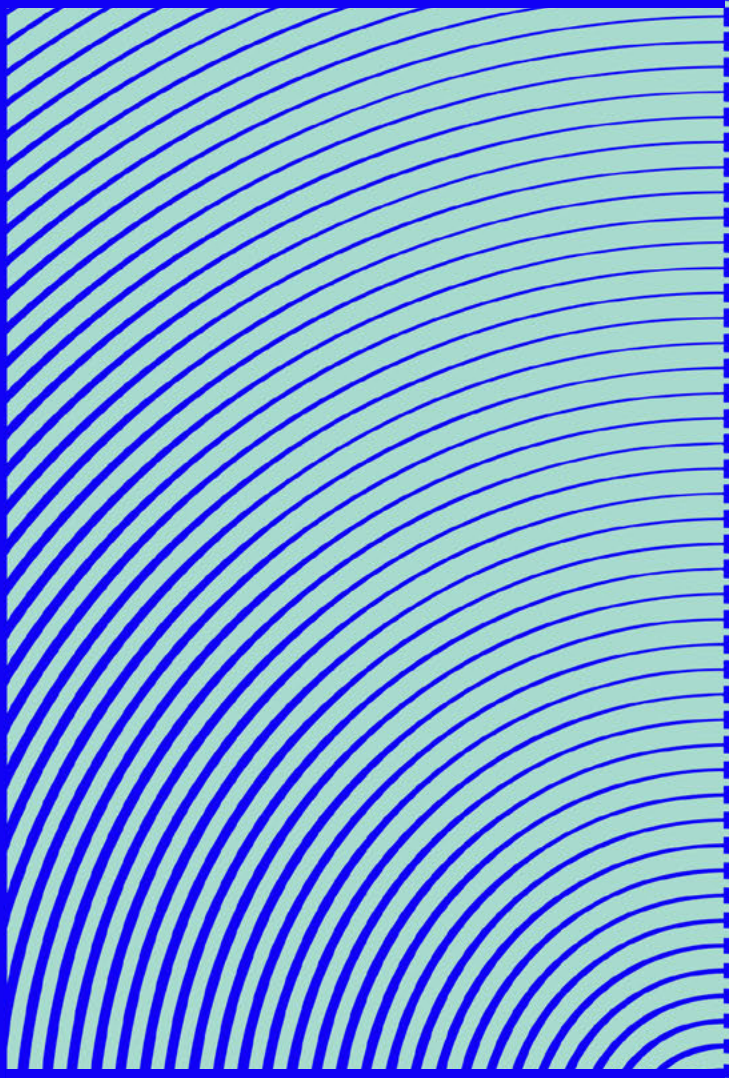
Access credentials to personal accounts are also valuable assets because they provide direct access to mailboxes, social media accounts, online shops, financial services and public administration information systems where additional sensitive information is stored. A wide range of valuable personal information 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.

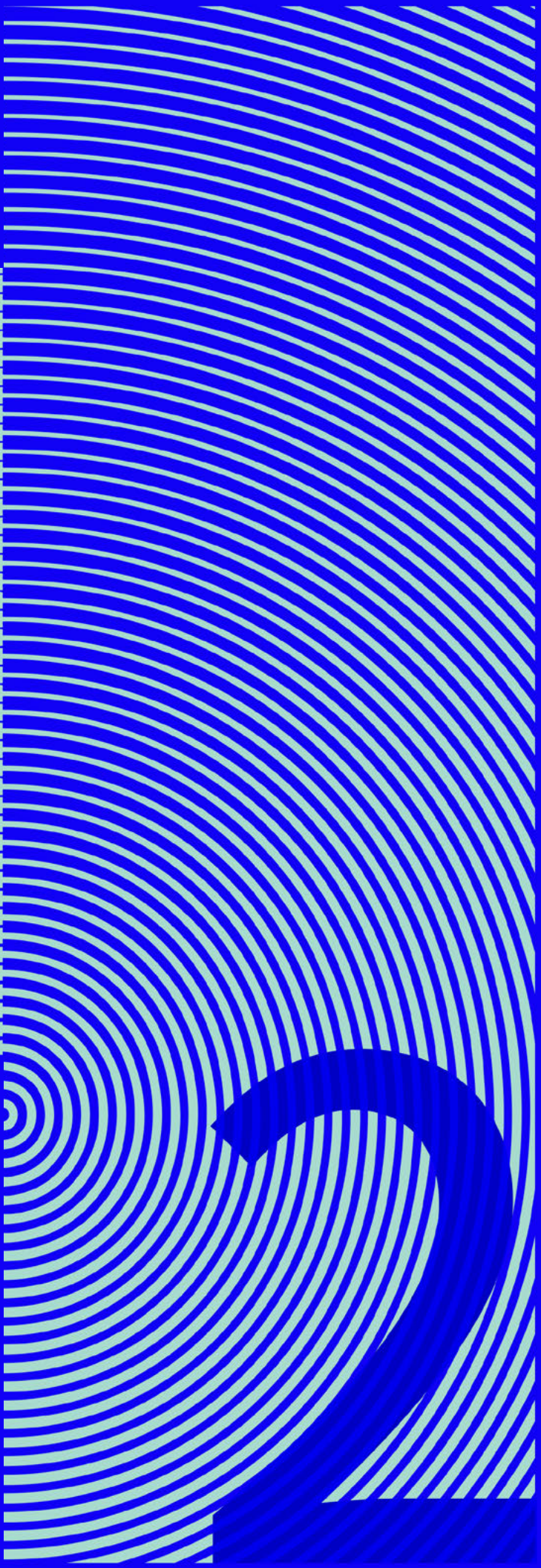
Access to a victim's account or system is the critical part of most cybercrime kill chains, as it can be used to compromise the wider network (lateral movement), distribute malware, steal sensitive information, impersonate the victim and/or use the account to distribute malicious content from a trusted 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.