



Organised crime online: How Europol disrupts cybercrime





Headquartered in The Hague, the Netherlands, Europol supports its Member States in preventing and combating all forms of serious international and organised crime, terrorism and cybercrime.

Fighting cybercrime is one of the agency's top priorities, as highlighted in the latest European Union Serious and Organised Crime Threat Assessment (EU-SOCTA). Within the EU-SOCTA, the following cybercrimes are considered key threats in the EU: cyber-attacks, online fraud schemes and (online) child sexual exploitation.

| Europol, Organised crime online: How Europol disrupts cybercrime

PDF Web | ISBN 978-92-9414-060-9 | DOI-10.2813/1796618 | QL-01-25-021-EN-N
PDF/X | ISBN 978-92-9414-061-6 | DOI-10.2813/3846074 | QL-01-25-021-EN-C

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

Luxembourg: Publications Office of the European Union, 2025

© European Union Agency for Law Enforcement Cooperation, 2025

Reproduction is authorised provided the source is acknowledged.


For any use or reproduction of photos or other material that is not under the copyright of Europol, permission must be sought directly from the copyright holders.

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

Cite this publication: Europol, Organised Crime Online: How Europol Disrupts Cybercrime, Publications Office of the European Union, Luxembourg, 2025.

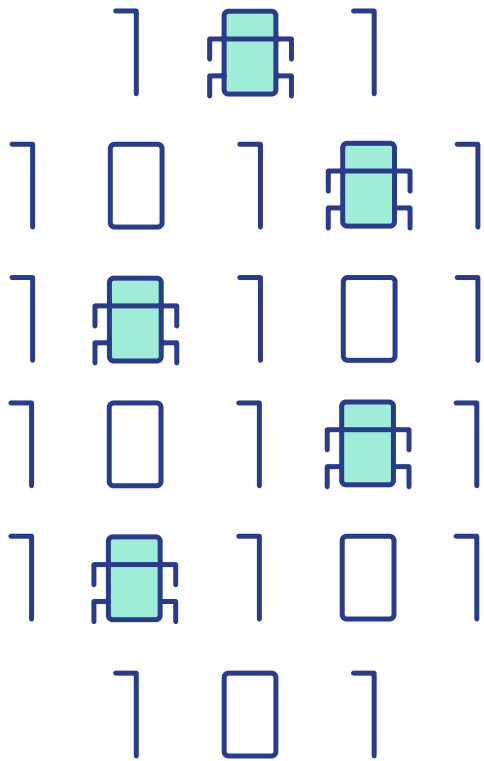
This publication and more information on Europol are available on the internet.

www.europol.europa.eu

 **Cyber-attacks** involve the online targeting of critical infrastructure, governments, businesses and private citizens by cybercriminals. They are often carried out on behalf of external threat actors, who are increasingly state-aligned and ideologically motivated.

Key trends in cyber-attacks:

- **Data is a central commodity in the malware threat landscape**, used for carrying out attacks, as a target, and as a by-product of attacks.
- **These crimes are enabled by the crime-as-a-service economy**, including dark web market forums selling stolen data, intrusion services, as well as criminal hosting and proxy providers.
- **The cybercrime landscape has become more fragmented**, with shorter life-spans and splintering of markets and ransomware groups, making identification of threat actors more challenging.



Targeting cybercrime networks

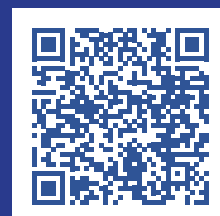
Operation Eastwood targeted cybercrime network NoName057(16). This joint internal operation with Eurojust took place between 14 and 17 July 2025.


Individuals acting for NoName057(16) are mainly Russian-speaking sympathisers who use automated tools to carry out distributed denial-of-service (DDoS) attacks. Operating without formal leadership or sophisticated technical skills, they are motivated by ideology and rewards.

National authorities have reached out to several hundred individuals believed to be supporters of this cybercrime network. The messages, shared via a popular messaging application, inform the recipients of the official measures highlighting the criminal liability they bear for their actions pursuant to national legislation.

This operation has so far resulted in the disruption of an attack infrastructure comprising 100 computer systems worldwide, and a significant portion of the group's central server infrastructure has been taken offline.

**You can access
the full IOCTA
report here**

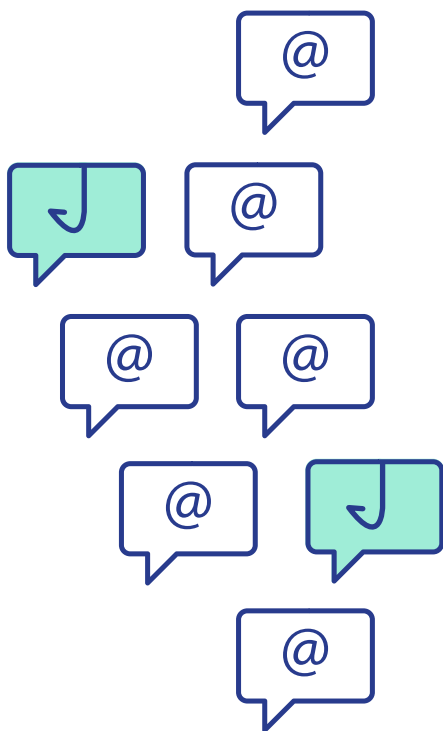


 **Online fraud schemes** constitute one of the most rapidly expanding sectors in organised crime, targeting a broad spectrum of victims. The scale of online fraud has reached an unprecedented magnitude and is projected to continue growing, driven by advancements in automation and AI.

Key trends in online fraud schemes:

- **Online fraud schemes** are becoming increasingly challenging to detect, as they tend to be long-lasting, tailor-made and highly sophisticated.
- **The theft of personal data from payment systems is a big concern.** Data is exploited directly or sold to other criminal actors, resulting in repeated victimisation of targets.
- **Some fraudsters display a high level of expertise** and continually develop their techniques, with future risks amplified by the attackers' adaptability.

The online fraud threat landscape features a well-organised and sophisticated criminal industry that not only targets victims, but also offers professional services to criminals. Fraudsters leverage advanced technologies, human behaviour, and gaps in legislation.



Investigating phishing-as-a-service platforms


Europol played a key role in disrupting one of the world's largest phishing-as-a-service platforms, LabHost. As part of the year-long operation, between 14 and 17 April 2024, there were a total of 70 addresses searched worldwide which resulted in the arrest of 37 suspects.

The LabHost platform offered, for a monthly subscription, a customisable service ranging from phishing kits to infrastructure hosting pages. Depending on the subscription, criminals were provided an escalating scope of targets from financial institutions, postal delivery services and telecommunication services providers, among others. This subscription also included a campaign tool named LabRat, which allowed unskilled criminals to monitor and control attacks in real time.

This operation has so far resulted in the uncovering of 40,000 phishing domains and over 10,000 users worldwide. Data collected from LabHost and LabRat will be used for ongoing international operational activities.

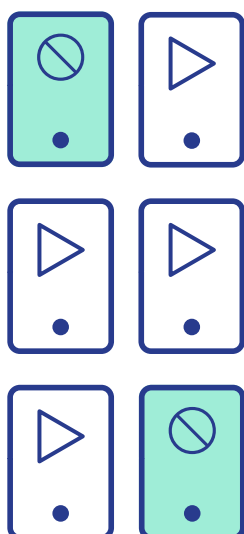
Listen to our podcast episode on how crime is nurtured online



 **Online child sexual exploitation (CSE)** refers to the sexual abuse of a person below the age of 18, as well as to the production and online sharing of images of such abuse. It is a heinous and severe crime as it involves physical and psychological violence on children, heavily impacting their health and development.

Key trends in CSE:

- **The digital acceleration has triggered a rapid evolution in online CSE.** It has provided borderless end-to-end encrypted platforms for offenders to create, store and exchange child sexual abuse material (CSAM), and to contact and groom victims.
- **The accessibility of AI tools has transformed the CSE landscape.** These tools can be used to edit existing material or create new content, for example making adults look younger in explicit images or turning non-explicit images into nude ones.
- **A variety of groups leverage digital platforms.** These are used to recruit offenders and victims on a global scale, normalise acts of extreme cruelty, extort victims, share CSAM, and even radicalise individuals into violent extremism.



Tackling child sexual exploitation

Operation Stream (also referred as “Operation Kidflix”) is one of the largest child sexual exploitation operations in Europol’s history. The investigation started in 2022 and resulted in action weeks from 10 to 23 March 2025.

Kidflix was created in 2021 and quickly became a popular platform among paedophiles. According to authorities, 91,000 unique videos were uploaded and shared, with a total running time of 6,288 hours. Unlike other platforms of this kind, Kidflix enabled users to download CSAM but also to stream video files. Users made payments using cryptocurrencies.

This operation has so far resulted in 1,393 suspects identified, 79 suspects arrested, over 3,000 electronic devices seized and 39 children protected.

To find out more about
cyber-attacks, online
fraud schemes and CSE,
you can access the
EU-SOCTA here



Changes in the cybercrime landscape: Exploitation of data

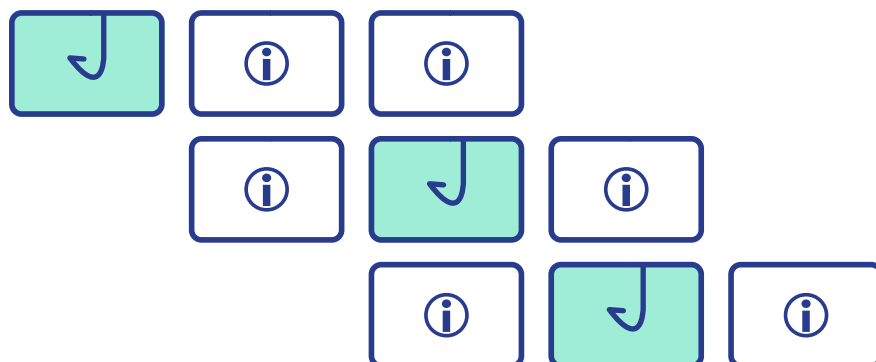
Over the past 12 months, Europol has continued to investigate the changing threats and trends within the cybercrime landscape. An overarching theme that emerged was the abuse of data as a driving force behind the criminal ecosystem ranging from online fraud, ransomware, to CSE. This was the central theme of this year's Internet Organised Crime Threat Assessment (IOCTA) **Steal, deal, and repeat: How cybercriminals trade and exploit your data.**

"You can't defend what you don't understand. Europol's IOCTA 2025 report sheds light on the hidden economy of stolen data that powers today's most dangerous cyber threats, giving law enforcement, policymakers, and industry the intelligence needed to act decisively."
Edvardas Šileris, Head of Europol's European Cybercrime Centre.

This year's findings highlight the following main trends that illustrate how cybercriminals are adapting their methods and expanding their operations:

➤ **Compromised data is 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. Social engineering stands out as a particularly prevalent technique.
- **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 advertise, negotiate and conduct sales transactions involving breached data, as well as to share the personal information of targeted victims, including children.



In focus:

Vectors used to harvest data

Cybercriminals use a variety of techniques that exploit either system vulnerabilities or human oversight to access and steal personal data. The use of social engineering techniques has become increasingly prevalent in data acquisition, some examples include:



Phishing

Type of attack that involves infecting victims with malware or tricking them into entering their credentials on fraudulent websites created using phishing kits.



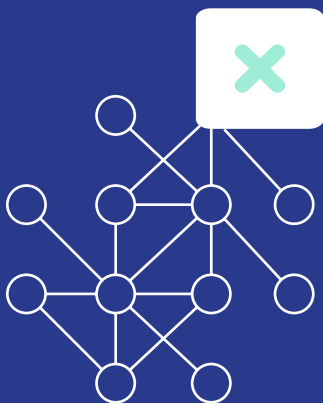
Infostealers

Category of malware specifically designed to illicitly extract sensitive information from compromised devices, collecting login credentials, application tokens and session cookies. Criminals use emails, SMS, or messages on social media with malicious attachments/URLs to introduce malware into the victim's system.



Vishing

Fraudulent phone calls tricking victims into providing sensitive information, enabled by spoofing¹ services, which allow criminals to impersonate local and reputable entities.



Disrupting botnets

Operation Endgame is part of a series of operations dedicated to disrupting botnets, making it one of the largest of its kind. It began in May 2024, and is currently ongoing.

Botnets are networks of devices that are infected with malware, allowing attackers to take remote control without the owners' knowledge. These malware infections usually begin with the use of droppers, a type of malicious software designed to install additional malware onto a targeted system.

Throughout its lifetime, Europol and the Joint Cybercrime Action Taskforce (J-CAT) have continued to support investigations by facilitating information exchange between the authorities involved, and providing analytical and forensic support to the investigators.

The latest Operation Endgame took place from 19 to 22 May 2025. During this period, authorities took down some 300 servers worldwide, neutralised 650 domains, and issued international arrest warrants against 20 targets, dealing a direct blow to the ransomware kill chain.

1. 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.



www.europol.europa.eu