IOCTA 2025

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle

Deputy Head of Section
Academy of European Law

Published in
2025, Vol. 20(2) eucrim
ISSN: 1862-6947
https://eucrim.eu

On 11 July 2025, Europol published the 10th edition of its 2025 Internet Organised Crime Threat Assessment (IOCTA). For the 2024 report →eucrim 2/2024, 123 with references to the previous years' reports.

Under the title "Steal, deal, and repeat: How cybercriminals trade and exploit your data", the 2025 IOCTA provides a detailed analysis of the significant developments, changes, and emerging threats in cybercrime in 2024. The report contains five chapters on the following central questions:

- Which data cybercriminals target?
- How they exploit it?
- How they acquire data and access?
- Who the criminal actors are?
- Where data and access are commodified?

The report emphasises the significant threat posed by data theft. Compromised data is highly valuable to a wide range of criminal actors, who exploit it both as a commodity in its own right and as a target to be acquired for other purposes, including the perpetration of further criminal activities. Cybercriminals use a variety of techniques to exploit both system vulnerabilities and human oversight in order to access and steal personal data.

Social engineering appears to be a particularly prevalent technique used. In addition, the efficacy of social engineering techniques increases with wider adoption of Large Language Models (LLMs) and other forms of generative artificial intelligence that enable more targeted communication with victims and the automation of criminal processes.

The sale of access to compromised systems and accounts is a thriving part of the criminal ecosystem. Consequently, Initial Access Brokers (IABs) are increasingly advertising these services, alongside related commodities, on specialised criminal platforms used by a wide range of cybercriminals. Looking at data brokers, the report finds that they are spreading their activities across multiple platforms in order to diversify their operations and increase their resilience against law enforcement operations. At the same time, 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.

In its conclusions, the report points out the need for multifaceted policy considerations that focus on both societal resilience and effective law enforcement within the EU's robust legal framework. According to the report, key actions should include the following:

- Lawful access by design to E2EE communication channels in cooperation with service providers and regulators.

- 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. This would involve targeting serious crimes and ensuring compliance with the principles of necessity and proportionality. Greater legal certainty would improve the effectiveness of cross-border investigations.
- The promotion of 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.

About eucrim

eucrim is the leading journal which regularly informs about current developments in European criminal and "criministrative" law.
All news items are freely accessible at: https://eucrim.eu/news/
Stay informed by emailing to eucrim-subscribe@csl.mpg.de to receive alerts for new releases of issues.
The project is co-financed by the Union Anti-Fraud Programme (UAFP), managed by the European Anti-Fraud Office (OLAF).

Co-funded by
the European Union