IOCTA 2024

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle

Deputy Head of Section
Academy of European Law

Published in
2024, Vol. 19(2) eucrim p 123
ISSN: 1862-6947
https://eucrim.eu

In July 2024, Europol published the 10th edition of its Internet Organised Crime Threat Assessment (IOCTA). For the 2023 report → eucrim 2/2023, 145-146.

The IOCTA 2024 offers an in-depth assessment of the key developments, changes, and emerging threats in cybercrime during the year 2023. The report's five chapters cover cryptocurrencies and the dark web, cyber-attacks, child sexual exploitation, online payments and fraud, and what to expect in the near future.

Millions of victims across the EU are attacked and exploited online on a daily basis, with small and medium-sized enterprises (SMEs) being increasingly targeted, as they tend to have fewer cyber defences. According to the report, the following were the biggest threats over the past year:

- An ever-growing volume of online child sexual abuse material (CSAM) including cases of AI-assisted, AI-altered ,and AI-generated CSAM;
- Investment, business email compromise (BEC), and romance fraud as well as digital skimming;
- AI-based tools and services becoming common tools for cybercriminals and a prominent commodity in the crime-as-a-service (CaaS) market, helping fraudsters to refine their social engineering capabilities;
- Ransomware groups splitting up and reorganising under different guises.

Key enablers of cybercrime include the dark web, cryptocurrencies and underground banking as well as cybercriminal abuse of legitimate end-to-end encryption (E2EE) messaging.

Looking at criminal actors, the report finds that the number of cybercriminals entering the market continues to grow steadily, comprising both lone actors and networks with various levels of expertise and capability. They operate from both within the EU and from third countries. Providers of ransomware-as-a-service (RaaS) compete for the services of high-level affiliates and developers, with some affiliates beginning to develop their own ransomware to lower their dependence on RaaS providers. Notably, the majority of criminals are young and unaware of the legal consequences of what they see as a mere challenge or game, even though their crimes have far-reaching implications for their own futures.

The report highlights the need for a renewed focus on offender prevention that addresses cybercrime at its core, leading to more sustainable and long-term solutions. It therefore recommends addressing the root causes that drive individuals to engage in cybercriminal activity, such as lack of awareness, financial incentives, and socio-economic factors. Cyber Offender Prevention (COP) is therefore seen as a key strategy, alongside investigative measures, in effectively combatting cybercrime.

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