IOCTA 2026

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle

Deputy Head of Section
Academy of European Law

Preprint eucrim 2026, Vol. 21(1)
ISSN: 1862-6947
https://eucrim.eu

On 28 April 2026, Europol published the 11th edition of its 2026 Internet Organised Crime Threat Assessment (IOCTA).

Under the title "The evolving threat landscape: how encryption, proxies and artificial intelligence are expanding cybercrime", the assessment provides a detailed analysis of significant developments, changes, and emerging threats in cybercrime in 2025. The report contains four chapters looking at cybercrime enablers, the criminal infrastructure behind online fraud schemes, cyber-attacks, and online child sexual exploitation.

Regarding cybercrime enablers, the report highlights how cybercriminals are adopting more resilient, anonymous, and sophisticated methods to evade detection and maintain their operations despite law enforcement efforts. Key developments include:

- Dark web marketplaces are increasingly fragmented, with many platforms specializing in specific criminal activities rather than offering a broad range of illicit services;
- Criminal marketplaces remain highly resilient, as new platforms quickly emerge and online forums enable the migration of users and vendors after disruptions;
- Cryptocurrencies remain the preferred payment method for ransomware attacks;
- The growing use of privacy-focused digital currencies and transaction-mixing services makes financial investigations more difficult;
- The distinction between the surface web and the dark web is becoming less clear as encrypted communication platforms and anonymous services increasingly connect both environments;
- Criminals exploit weaknesses in the domain name registration process by using newly registered domains before law enforcement agencies can detect and disrupt them;
- Cybercriminals are deploying increasingly complex technical infrastructures, including multilayered hosting arrangements, anonymous routing techniques, and residential proxy networks.

In the area of criminal infrastructure behind online fraud schemes, the report warns that online fraud is becoming more sophisticated, scalable, and difficult to detect, driven by evolving criminal infrastructures and the growing use of advanced technologies.

- Online fraud schemes continue to expand;
- Phishing remains one of the most common fraud methods;
- The misuse of subscriber identity module box devices enables criminals to conduct large-scale attacks through mass communication and identity spoofing;
- Some criminal groups are moving away from commercial hosting providers and building their own infrastructure to avoid identity verification requirements;
- The theft of digital assets has evolved into a crime-as-a-service model;

- Generative artificial intelligence is helping fraudsters create more convincing and personalized scams;
- Autonomous artificial intelligence systems are expected to automate parts of the criminal process and significantly increase the scale and effectiveness of online fraud.

Regarding cyber-attacks, the report highlights a ransomware ecosystem that is becoming more fragmented, competitive, and adaptable, with criminal groups continuously evolving their methods and services.

- The ransomware landscape remains highly volatile, with new ransomware brands emerging due to competition among criminal groups, law enforcement disruptions, and access to new technologies;
- Ransomware attacks continue to increase, with more than 120 active ransomware brands observed during 2025;
- Ransomware-as-a-service groups are expanding their offerings to attract affiliates, including the integration of artificial intelligence tools and more customizable services;
- Significant overlaps exist between different ransomware operations, as affiliates and administrators often work across multiple brands and campaigns;
- Affiliates and administrators play a central role in sustaining and expanding the ransomware ecosystem, contributing to its resilience despite enforcement actions;
- Hybrid threat actors increasingly use cybercriminal networks as proxies to conduct distributed denial-of-service attacks, ransomware operations, data theft campaigns, and attacks against strategically important targets.

Lastly, the report highlights an increasingly complex and harmful landscape of online child sexual exploitation, driven by financial incentives, new technologies, and secure communication platforms.

- Extortion remains a major component of child sexual exploitation, with victims coerced into sending money, producing additional sexual material, or engaging in harmful and abusive acts under threat;
- The trade in child sexual abuse material for financial gain is increasing, alongside a persistent threat from live-distant child abuse and a growing number of scam platforms involved in selling or distributing such material;
- The emergence of artificially generated child sexual abuse material is creating additional challenges for detection, victim identification, and law enforcement investigations;
- End-to-end encrypted messaging applications are widely used by offenders for grooming, sharing illegal material, and coordinating activities due to the difficulty authorities face in accessing communications;
- Criminal networks are exploiting both financial incentives and technological tools to expand the scale, reach, and concealment of child sexual exploitation activities.

Looking ahead, the report warns of a future in which cybercrime becomes increasingly automated through advanced artificial intelligence systems capable of carrying out criminal activities with minimal human involvement. Cybercriminal groups are expected to become more resilient and harder to identify, while collaborations between state-linked actors and criminal networks may intensify cyber threats against governments, businesses, and critical infrastructure. Online fraud is likely to grow in scale and sophistication as artificial intelligence enables highly convincing scams and automates criminal operations. The spread of synthetic child sexual abuse material, combined with the wider use of end-to-end encryption and decentralized platforms, is expected to create significant challenges for law enforcement. Criminals are also likely to continue exploiting cryptocurrencies, offshore financial services, and fintech platforms to move and conceal illicit funds.

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