The Current Cybercrime Landscape: IOCTA 2019

Cornelia Riehle

eucrim
European Law Forum: Prevention • Investigation • Prosecution

News

AUTHOR

Cornelia Riehle
Deputy Head of Section
Academy of European Law

ISSN: 1862-6947
https://eucrim.eu

On 9 October 2019, Europol published its 2019 Internet Organised Crime Threat Assessment (IOCTA). The 2019 IOCTA provides key findings and recommendations regarding the cybercrime threat landscape, focusing on six crime priorities:

- Cyber-dependent crime;
- Online child sexual exploitation;
- Payment fraud;
- Criminal abuse through the Darknet;
- The convergence of cybercrime and terrorism;
- Cross-cutting crime factors.

Looking at cyber-dependent crime (meaning any crime that can only be committed using computers, computer networks, or other forms of information communication technology), the overall volume of ransomware attacks has declined. Attackers seem to focus on fewer but more profitable targets. Nevertheless, ransomware remains the most significant threat in the field of cybercrime. In its recommendation on how to tackle cyber-dependent crime, the report finds that targeting major crime-as-a-service-providers is the most successful approach. Furthermore, the report recommends the following:

- Strong cooperation between law enforcement and the private sector;
- Collaboration between the network and information security sector and cyber law enforcement authorities;
- The use of existing cooperation channels.

Low-level cybercrimes should also be targeted as a means of intervention in the criminal careers of young, developing cybercriminals.

As regards child sexual exploitation online, the report finds a continued increase in available child sexual exploitation material (CSEM), self-generated explicit material (SGEM), and even live distant child abuse (LDCA). In order to reduce CSEM material, the report recommends coordinated action with the private sector and the deployment of new technology, a structural educational campaign across Europe, and law enforcement cooperation with developing countries. One concrete measure to prevent child sex offenders from travelling to third countries to sexually abuse children would be the use of passenger name record (PNR) data by EU law enforcement authorities (accessible through the Travel Intelligence team within Europol).

In the area of payment fraud, the report sees CNP (card not present) fraud as the main priority; however, skimming also continues to evolve as do jackpotting attacks. To combat payment fraud, the report recom-

mends cooperation between the public and private sectors, the exchange of information, training of employees, and raising awareness among customers.

The report emphasizes the key role of the Darknet in the increasing number of single-vendor shops and smaller, fragmented markets as an enabler of trade in an extensive range of criminal products and services. To combat criminal abuse through the Darknet, the report identifies the following measures as key:

- Coordinated investigation and prevention actions;
- The ability to maintain accurate real-time information;
- Improved coordination and standardisation of undercover online investigations;
- An EU-wide legal framework to clarify jurisdiction despite anonymity issues.

Challenges with regard to the convergence of cybercrime and terrorism include the wide array of online service providers (OSPs) and the use of new technologies being exploited by terrorist groups. To counter terrorist groups' online propaganda and recruitment operations, the report recommends addressing the entire spectrum of abused OSPs. In order to manage a crisis after a terrorist attack, the report emphasizes the need for cross-platform collaboration and a multi-stakeholder crisis response protocol on terrorist content online.

New cross-cutting crime factors include hackers and fraudsters now routinely targeting crypto-assets and enterprises. In order to tackle these factors, the report recommends that law enforcement develop and share knowledge with the judiciary, establish relationships with cryptocurrency-related businesses, and share information with Europol.

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