IOCTA 2020

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 5 October 2020, Europol published its Internet Organised Crime Threat Assessment (IOCTA) 2020. The report details the latest developments with regard to cross-cutting crime facilitators and challenges to criminal investigations, cyber-dependent crime, child sexual exploitation online, payment fraud, and criminal abuse via the dark web.

In the area of cross-cutting crime, the report finds that social engineering remains an effective threat that enables other types of cybercrime. Cryptocurrencies continue to facilitate payments for various forms of cybercrime with developments towards privacy-oriented crypto coins and services. The report also describes reporting challenges that hinder the rendering of an accurate overview of crime prevalence across the EU.

As in the 2019 IOCTA report, the 2020 report identifies ransomware as the most dominant threat in the field of cyber-dependent crime with criminals threatening the victims to publish data if they do not pay. Furthermore, ransomware targeting third-party providers also creates significant potential damage for other organisations in the supply chain and critical infrastructure. The malware 'Emotet' is omnipresent, given its versatile use, and it is the benchmark of modern malware. Lastly, the report sees a high threat potential of DDoS attacks.

Looking at online child sexual exploitation (CSE), the report sees a continuing trend (see also IOCTA 2018 and IOCTA 2019) of an increasing amount of online child sexual abuse material (CSAM), being further exacerbated by the COVID-19 crisis. Consumption is reinforced by the enhanced use of encrypted chat apps and similar offers, which makes it more difficult for law enforcement to detect and investigate online child sexual exploitation activities. Furthermore, online offender communities exhibit considerable resilience and are found to be continuously evolving. The commercialisation of online CSE is becoming an increasingly widespread issue, with livestreaming of child sexual abuse continuing to increase and becoming even more prevalent during the COVID-19 crisis.

In the area of payment fraud, the report pinpoints online investment fraud as one of the most rapidly growing crimes, generating millions in losses and affecting thousands of victims. SIM swapping seems to be a key trend. Furthermore, business email compromise (BEC) remains an area of concern, and card-not-present (CNP) fraud continues to increase.

Ultimately, the report describes the dark web environment as volatile, with lifecycles of dark web marketplaces being shorter and no new, clearly dominant market arising compared to previous years to fill the vacuum left by the takedowns in 2019. However, the nature of the dark web community at the administrator level also shows how adaptive it is in challenging times, leading to more effective cooperation in the search for better security solutions and safe dark web interaction.

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