INTERNET ORGANISED CRIME THREAT ASSESSMENT (IOCTA)

Strategic, policy and tactical updates on the fight against cybercrime

ABOUT IOCTA UPDATES

IOCTA 2019 report (PDF)

All IOCTA reports

Each year, Europol's European Cybercrime Centre (EC3) publishes the Internet Organised Crime Threat Assessment (IOCTA), its flagship strategic report on key findings and emerging threats and developments in cybercrime — threats that impact governments, businesses and citizens in the EU.

The IOCTA provides key recommendations to law enforcement, policy makers and regulators to allow them to respond to cybercrime in an effective and concerted manner.

The report focuses on the crime areas that fall under EC3's mandate. These cybercrime priorities, which are determined by the EU Policy Cycle - EMPACT, are currently:

- Cyber-dependent crime
- Online child sexual exploitation
- Payment fraud

The most recent IOCTA also looks at an additional crime area, online criminal markets, both on the surface web and Darknet. It also addresses the convergence of cyber and terrorism.

Another typical focus of the IOCTA are cross-cutting crime enablers, factors that straddle more than one crime area but are not necessarily inherently criminal themselves. These enablers include:

- phishing/smishing/vishing
- business email compromise
- bulletproof hosting
- anonymisation tools
- criminal abuse of cryptocurrencies
- money muling.

STRUCTURE

While there have been variations in how each IOCTA is put together, the basic structure is fairly constant. Each of the main chapters

- describes the key findings on a particular cybercrime area in the reporting year;
- identifies future trends and developments;
- makes recommendations.

In addition, the IOCTA contains a brief summary of geographic threats and cybercrime activity throughout the five continents.

Each issue draws on contributions from:

- experts at Europol
- EU Member States
- law enforcement authorities both within and outside the EU
- partners in private industry, the financial sector and academia.
The IOCTA may also include word on operational successes in the year under review. Two examples will serve as illustrations.

The first is the takedown of one of the largest marketplaces for hiring DDoS services, webstresser.org. With 150 000 registered users, the site was the source of 4 million DDoS attacks. Operation Power OFF was led by the Dutch Police and the UK’s National Crime Agency, supported by Europol and a dozen law enforcement authorities from around the world.

The second is the increased cooperation between law enforcement. In 2019, law enforcement shut down two of the most prolific dark web marketplaces, Wall Street Market and Valhalla. At the time of its closure, Wall Street had over 1 150 000 users and 5 400 vendors.