JOINT CYBERCRIME ACTION TASKFORCE (J-CAT)

Fighting cybercrime around the world

Cybercrime knows no boundaries. Cybercriminals are constantly coming up with new ways to profit from their crimes at the expense of citizens, businesses and governments, across national borders and jurisdictions.

Police forces around the world thus encounter similar cybercrimes and similar criminal targets, and that calls for a coordinated, international approach to the problem.

The Joint Cybercrime Action Taskforce (J-CAT), which was launched in September 2014, fills that need. Located at Europol's European Cybercrime Centre (EC3), it helps fighting cybercrime within and outside the EU.

It consists of a standing operational team of cyber liaison officers from several EU Member States and non-EU cooperation partners, who are based in Europol headquarters and complemented with EC3 staff. The cyber liaison officers come from:

- committed and closely involved EU Member States (Austria, France, Germany, Italy, the Netherlands, Romania, Poland, Spain and Sweden);
- non-EU law enforcement partners (Australia, Canada, Colombia, Norway, Switzerland, United Kingdom and the United States, which is represented by two agencies: the Federal Bureau of Investigation and Secret Service);
- EC3.

All these officers work from the same office to ensure that they can communicate with each other easily.

In addition, national experts seconded from Europol to Eurojust regularly cooperate with EC3 and attend the weekly J-CAT meetings to discuss cases and projects of mutual interest. J-CAT chooses and prioritises which cases to pursue based, among other things, on proposals from the country liaison officers. Members:

1. select the most relevant proposals;
2. share, collect and enrich data on the cases in question;
3. develop an action plan, which is led by the country that submitted the selected proposal;
4. go through all the necessary steps to ensure the case is ready to become a target of law enforcement action — a process that involves consulting with judicial authorities, the identification the required resources and the allocation of responsibilities.

The taskforce was also involved in several of the operations outlined in the latest Internet Organised Crime Threat Assessment (IOCTA), thus contributing significantly to their success.

An example of an action that was coordinated by Europol and the Joint Cybercrime Action Taskforce (J-CAT) with the support of the Dutch Politie and the British National Crime Agency was the operation and the arrest of the administrators and the shutdown of the DDoS marketplace webstresser.org on April 2018. The orchestrated attacks targeted critical online services offered by banks, government institutions and police forces, as well as victims in the gaming industry.
The UK’s South East Regional Organised Crime Unit (SERCU), in a joint operation with the Hessen State Police in Germany, the UK’s National Crime Agency (NCA) and Europol, has arrested a 36 year-old individual on suspicion of fraud, theft and money laundering. The operation was launched following the theft of around €10 million in the IOTA cryptocurrency from over 85 victims worldwide since January 2018.

A 25 year-old coder was arrested on 18 May 2018 by the Royal Thai Police based on a French international arrest warrant. The coder helped extort a British company after compromising a large amount of customer data. The arrest of this young cybercriminal was the eight in an international operation supported by Europol and the Joint Cybercrime Action Taskforce (J-CAT) that started exactly one year ago. This case illustrates that cyber-related extortion remains a common tactic among cybercriminals, as identified in the recent IOCTA reports.

Source URL: https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce