FRENCH CODER WHO HELPED EXTORT BRITISH COMPANY ARRESTED IN THAILAND
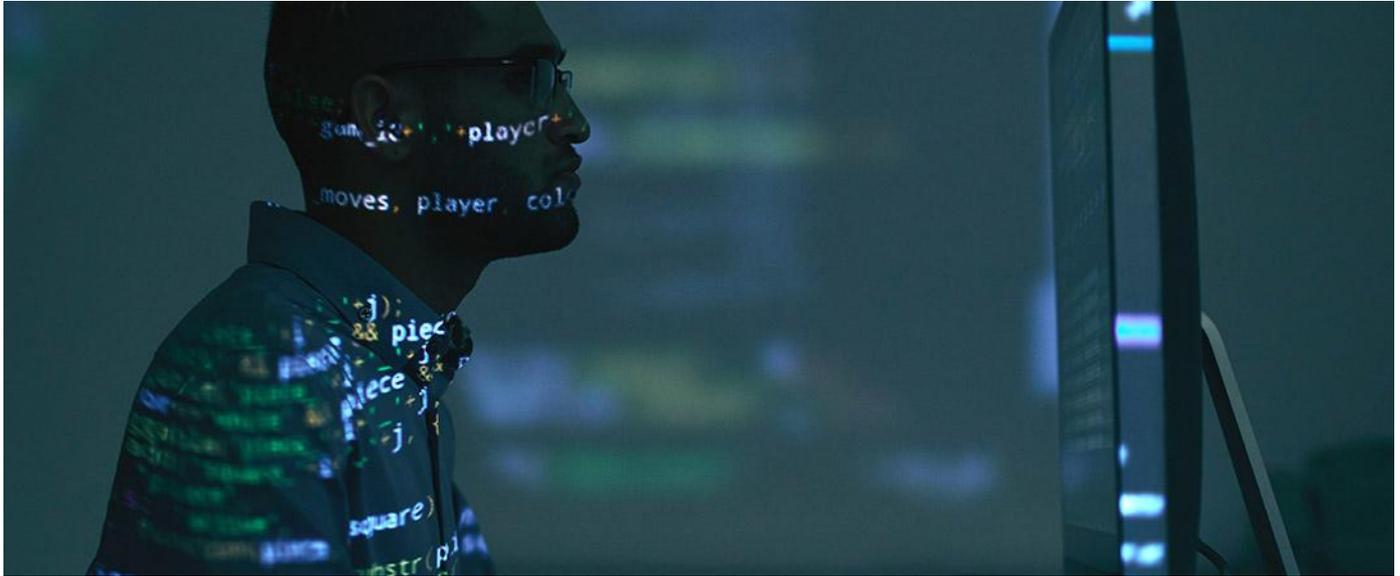
14 Jun 2018
Press Release
International cooperation was key to success

A 25-year-old coder was arrested on 18 May by the Royal Thai Police based on a French international arrest warrant. 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.

In May 2017 a British-based company was the victim of a cyber-attack during which a large amount of customer data was compromised. The attack was immediately claimed by an organisation called Rex Mundi. A few days later, the company received a phone call from a French-speaking person explaining that he was a member of Rex Mundi. This person shared a large number of credentials with the company to prove that they had access to the data. He also demanded ransom of either almost EUR 580 000 for the non-disclosure of the customer data or over EUR 825 000 for information on the security breach and how to handle it. For each day the company failed to pay, there would be a ransom of EUR 210 000. The ransom was to be paid in Bitcoin.

Based on information from the Metropolitan Police in the UK, the French National Police (High Tech Crime Unit Central Office OCLCTIC-DCPJ) and Europol were informed and an intense international cooperation started. Within an hour, Europol's 24/7 Operational Centre was able to link the available information to a French national. Five people were arrested in June 2017 by the French authorities. The main suspect admitted his involvement in the blackmail but hired the services of a hacker on the dark web to carry out the cyber-attack. The French National Police arrested two hackers in France in October 2017 and a final accomplice, also a French national with coding skills, was recently apprehended in Thailand.

This case illustrates that cyber-related extortion remains a common tactic among cybercriminals, as identified in the IOCTA 2017. As indicated in the report, for such financially motivated extortion attempts, attacks are typically directed at medium-sized or large enterprises, with payment almost exclusively demanded in Bitcoins.

This operation was financed by EMPACT. In 2010 the European Union set up a four-year Policy Cycle to ensure greater continuity in the fight against serious international and organised crime. In 2017 the Council of the EU decided to continue the EU Policy Cycle for the 2018 - 2021 period. This Policy Cycle aims to tackle the most significant threats posed by organised and serious international crime to the EU. Cybercrime is one of the priorities for the Policy Cycle.

CRIME AREAS	Cybercrime
TARGET GROUPS	General Public · Law Enforcement · Academia · Professor · Students · Researcher · Press/Journalists · Other
GENERAL TERMS	EU Police Cycle (EMPACT)
ENTITIES	European Cybercrime Center (EC3)
SUPPORT & SERVICES	Operational coordination · Operational support · Information exchange