EMPACT

EUROJUST

12 cyber criminals targeted for involvement in international ransomware attacks

26-27 October 2021 – **12 individuals**, under investigation in several high-profile cases in different jurisdictions, **are targeted in a joint operation** involving Ukraine, Switzerland, France, the Netherlands, Norway and the United States. **More than 50 foreign investigators**, including six Europol specialists, are deployed to Ukraine to assist with the joint action. Over USD 52 000 in cash and 5 luxury cars are seized, as well as electronic devices for forensic examination to secure further evidence and identify new investigative leads.

2019–2021 – A total of **seven coordination meetings** are held at Eurojust to facilitate the cross-border **judicial cooperation** and **information exchanges**. Europol provides **digital forensic support** and **cyber intelligence**, while also hosting a series of operational meetings.

September 2019 – Initiated by the French authorities, a **joint investigation team (JIT)** is set up between **France**, **Norway** and the **United Kingdom**, with **Ukraine** joining in January 2020, to uncover the magnitude and complexity of the crimes committed and to establish a joint strategy. The JIT receives financial backing from Eurojust and operational assistance from both Eurojust and Europol. Partners to the JIT collaborate closely with counterparts leading parallel independent investigations in **the Netherlands** and the **United States**.

February 2019 – A **case is opened at the initiative of the French Desk at Eurojust**, which over the course of the investigation involves **three Member States**, **five third countries** with Liaison Prosecutors posted at Eurojust, and **Europol**.

Discovered in 2019, a highly organised criminal network applies various means (including *LockerGoga* and *MegaCortex* ransomware) to compromise IT systems worldwide. These entail brute force attacks, SQL injections, stolen credentials and phishing emails with malicious content. The malware remains undetected in the compromised systems, sometimes for months, thereby magnifying its spread even further. The criminals target mainly large corporations, effectively bringing many businesses to a halt. Ransom notes demand that the attackers be paid in bitcoin in exchange for decryption keys.The effects of the attacks, occuring in no less than 71 countries, are devastating to many of the victims.