# International operation targets cyber criminals for worldwide 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.

# 12. Cybercrime

Criminal online activities have recently become much bolder and grown in frequency and number, defrauding private individuals and legitimate enterprises. The COVID-19 pandemic has significantly boosted online communications, and criminal networks have stepped up their illicit activities to abuse the internet for large-scale fraudulent schemes.

Eurojust's cybercrime activities spanned many areas in 2021, including ransomware, artificial intelligence, encryption, and cybercrime as a service. Cybercrime products published by Eurojust in 2021 include: the Cybercrime Judicial Monitor, the EU Digital Evidence Situation Report, and the Third report of the observatory function on encryption.

## 12.1 Ransomware

As the digitalisation of society continues, creating more connections among people, businesses and governmental structures, our vulnerability to cyberattacks is increasing, as is the possibility of a full-scale horizontal impact in several EU jurisdictions at the same time. Ransomware groups are increasingly sophisticated, act strategically to maximise profits and reduce risks, and use multilayers of extortion methods to pressure victims and cooperate with other malware criminal groups.

In 2021, the EJCN gathered all its learnings on this priority topic in the EJCN Map of Ransomware, providing an overview of answers to the Network's questionnaire from the EU Member States, as well as Norway and Switzerland. The analysis demonstrates that the level of awareness on ransomware from law enforcement and judicial authorities remains low, and the ability to respond to it greatly varies across Europe. This exercise, in cooperation with Eurojust, is a starting point for the Network to support greater efficiency in fighting ransomware by providing proper tools for judicial authorities to tackle it.

Following a joint EU-US statement in June 2021 underlining the need for cooperation, the topic has also been discussed in high-level meetings between the European Union and the United States. On 25 October 2021, Eurojust participated in the first meeting of the newly established EU-US Ransomware Working Group, dedicated to ransomware issues focusing on operational aspects. The Working Group will collaborate on international issues in an effort to mitigate ransomware threats impacting both the United States and the European Union.


**CYBERCRIME CASES IN 2021**

**398** CASES
(188 *new cases*, 210 *ongoing from previous years*)

**16**
JOINT INVESTIGATION TEAMS
(3 *new JITs*, 13 *ongoing*)

**66**
CASE-SPECIFIC COORDINATION MEETINGS

**5**
COORDINATED ACTION DAYS

As a follow-up, Eurojust President Ladislav Hamran, was invited to present the judicial dimension of the EU-US cooperation on ransomware at the EU-US JHA Ministerial Meeting in December 2021. He stressed that the increase in the number of ransomware attacks, particularly in healthcare during the pandemic, creates important questions for prosecutors and judges. For example, should crime groups attacking healthcare facilities be considered as not only having illicit profit-making in their intent but also the intent to cause physical harm to people, or even murder?

In 2022, Eurojust looks forward to hosting a high-level workshop with its US partners to further translate the joint fight against ransomware into operational outcomes. Moreover, the Agency's new ransomware subgroup within Eurojust's Cybercrime Working Group will monitor legislative developments and provide strategic guidance in the field.

## 12.2 Artificial intelligence

Artificial intelligence is gaining importance in criminal law and is being used increasingly by the police and judicial authorities in criminal matters. In April 2021, the European Union published a new Proposal for a Regulation on laying down harmonised rules on Artificial Intelligence. In view of the proposed

Photos © Shutterstock

Regulation, and to keep abreast of legislative developments in this area, Eurojust has recently set up a dedicated AI group within its Cybercrime Working Group.

Furthermore, the Agency is a member of the multi-agency Innovation Hub for Internal Security, which provides a joint platform to support the delivery of cutting-edge technologies for the security of citizens in the European Union. In April 2021, Eurojust contributed to a project launched by the Innovation Hub, aimed at developing accountability principles to guide human-centred and socially driven AI capabilities for security and justice organisations. The project aims to create a toolkit for practitioners to auto-evaluate future AI systems in light of the accountability principles.

## 12.3 Latest developments from the European Judicial Cybercrime Network (EJCN)

The EJCN, supported by Eurojust, consists of a network of judicial authorities specialised in countering the challenges of cybercrime, cyber-enabled crime and investigations in cyberspace. In 2021, EJCN participants discussed current criminal trends and analysed cases to improve future cybercrime investigations. Based on these experiences, the Network analysed the judiciary's training needs to provide short specialised trainings during 2022. In addition to this, the EJCN contributed to Eurojust's Cybercrime Judicial Monitor, covering legislative developments in the areas of cybercrime, cyber-enabled crime and electronic evidence.

At its 10th Plenary Meeting in June 2021, the EJCN presented its new Virtual Currency Guide for Judicial Authorities. Virtual currencies are becoming increasingly popular with criminals. They use them to pay for illegal services and goods or to buy them themselves, while hiding and laundering the proceeds of their illegal activities through virtual currencies.

In the current digital age, the emergence of these virtual currencies creates serious challenges for judicial and law enforcement authorities in investigating crimes that involve their use. Considering that most countries do not have specific criminal legal provisions in this area, the Guide offers tailor-made advice for prosecutors dealing with virtual currencies.

During the Plenary meeting, practitioners also discussed the topic of cybercrime as a service and possible strategies to support victims in complex cybercrime cases.

In its most recent meeting, held in December 2021, the EJCN discussed challenges and best practices in the investigation of ransomware cases, with a special focus on the healthcare sector. The Network addressed the issue of how to better connect with the private sector to increase the efficiency of cybercrime criminal investigations. Possible synergies with third countries in relation to cybercrime and digital evidence were also discussed in the framework of EuroMed's subgroup on digital evidence.

## 12.4 Case examples illustrating Eurojust's work on cybercrime

### Access to VPN service used by ransomware groups cut off

**CRIME**: DoubleVPN was a virtual private network (VPN) service which provided a safe haven for cybercriminals to attack their victims. It was advertised as a means to mask the location and identities of ransomware operators and phishing fraudsters, providing a high level of anonymity by offering VPN connections to its clients.

**ACTION**: During an action day in June 2021, law enforcement and judicial authorities in Europe, the United States and Canada seized DoubleVPN's web domains and server infrastructure. The Dutch authorities leading the case instigated a digital intrusion of the infrastructure that facilitated the gathering of evidence against DoubleVPN and its users.

**RESULT**: Servers hosting DoubleVPN content were seized across the world and the web domains were replaced with a law enforcement splash page.

**EUROJUST'S ROLE**: Eurojust facilitated the judicial cross-border cooperation leading to the takedown of the network. The Agency organised six dedicated coordination meetings, aimed, inter alia, at verifying and solving legal issues related to the collection of data in the countries concerned, and set up a coordination centre through which the operation was implemented on the ground by the various national authorities involved.

### Major fraudulent German investment platform taken down

**CRIME**: A major fraudulent online German investment platform defrauded victims of at least EUR 15 million. After initial investments, victims were encouraged to pay more into the alleged investment fund, losing all of their money.

**ACTION**: During an action day in October 2021, the main suspect was arrested and eight places were searched.

**RESULT**: The fraudulent online investment platform was dismantled by the authorities in Germany, Bulgaria, Cyprus, the Netherlands and Ukraine, and supported by Eurojust and Europol.

**EUROJUST'S ROLE**: Eurojust set up a coordination centre and assisted with the exchange of cross-border judicial information between all countries involved. The Agency also provided support for the execution of EAWs. authorities involved.