RANSOMWARE GANG ARRESTED IN UKRAINE WITH EUROPOL'S SUPPORT

04 October 2021
Press Release

On 28 September, a coordinated strike between the French National Gendarmerie (Gendarmerie Nationale), the Ukrainian National Police (Національна поліція України) and the United States Federal Bureau of Investigation (FBI), with the coordination of Europol and INTERPOL, has led to the arrest in Ukraine of two prolific ransomware operators known for their extortionate ransom demands (between €5 to €70 million).

Results of the action day

2 arrests and 7 property searches
Seizure of US$ 375 000 in cash
Seizure of two luxury vehicles worth €217 000
Asset freezing of $1.3 million in cryptocurrencies

The organised crime group is suspected of having committed a string of targeted attacks against very large industrial groups in Europe and North America from April 2020 onwards. The criminals would deploy malware and steal sensitive data from these companies, before encrypting their files.

They would then proceed to offer a decryption key in return for a ransom payment of several millions of euros, threatening to leak the stolen data on the dark web should their demands not be met.

Close cooperation between the involved law enforcement authorities, supported by Europol's Joint Cybercrime Action Taskforce (J-CAT), led to the identification in Ukraine of these two individuals.

Six investigators from the French Gendarmerie, four from the US FBI, a prosecutor from the French Prosecution Office of Paris, two specialists from Europol's European Cybercrime Centre (EC3) and one INTERPOL officer were deployed to Ukraine to jointly conduct investigative measures with the National Police.

Europol supported the investigation from the onset, bringing together all the involved countries to establish a joint strategy. Its cybercrime specialists organised 12 coordination meetings to prepare for the action day, alongside providing analytical, malware, forensic and crypto-tracing support. A virtual command post was set up by Europol to ensure seamless coordination between all the authorities involved.

The following law enforcement authorities took part in this investigation:

France: National Cybercrime Centre of the National Gendarmerie (C3N)
Ukraine: Cyber Police Department of the National Police of Ukraine
United States: Atlanta Field Office of the Federal Bureau of Investigation
Europol: European Cybercrime Centre (EC3)
INTERPOL : Cyber Fusion Centre

This operation was carried out in the framework of the European Multidisciplinary Platform Against Criminal Threats (EMPACT).