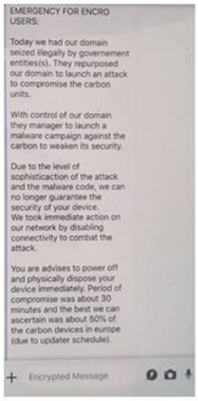
DISMANTLING OF AN ENCRYPTED NETWORK SENDS SHOCKWAVES THROUGH ORGANISED CRIME GROUPS ACROSS EUROPE

02 July 2020

Press Release

Europol/Eurojust joint press release



At a joint press conference today, French and Dutch law enforcement and judicial authorities, Europol and Eurojust have presented the impressive results of a joint investigation team to dismantle EncroChat, an encrypted phone network widely used by criminal networks.

Over the last months, the joint investigation made it possible to intercept, share and analyse millions of messages that were exchanged between criminals to plan serious crimes. For an important part, these messages were read by law enforcement in real time, over the shoulder of the unsuspecting senders.

The information has already been relevant in a large number of ongoing criminal investigations, resulting in the disruption of criminal activities including violent attacks, corruption, attempted murders and large-scale drug transports. Certain messages indicated plans to commit imminent violent crimes and triggered immediate action. The information will be further analysed as a source of unique insight, giving access to unprecedented volumes of new evidence to profoundly tackle organised criminal networks.

In recent years, European countries have been increasingly affected by organised crime groups who are pervasive and highly adaptive, posing one of the most pressing security challenges faced by law enforcement and judicial authorities. In this regard, the abuse of the encrypted communication technologies is a key facilitator of their criminal activities.

Since 2017, the French Gendarmerie and judicial authorities have been investigating phones that used the secured communication tool EncroChat, after discovering that the phones were regularly found in operations against organised crime groups and that the company was operating from servers in France. Eventually, it was possible to put a technical device in place to go beyond the encryption technique and have access to the users' correspondence.

In early 2020, EncroChat was one of the largest providers of encrypted digital communication with a very high share of users presumably engaged in criminal activity. User hotspots were particularly present in source and destination countries for cocaine and cannabis trade, as well as in money laundering centres.

Given the widespread use of the encrypted telephone solution by EncroChat among international criminal networks around the world, French authorities decided to open a case at Eurojust, the EU Agency for Criminal

Justice Cooperation, towards the Netherlands in 2019. Further developments in the investigations led to organising the processing of the data, which was captured on the basis of the provisions of French law and with judicial authorisation, through the frameworks for international judicial and law enforcement cooperation.

The data was in first instance shared with the Netherlands. Eurojust facilitated the creation of a joint investigation team (JIT) between the two countries and with the participation of Europol, the European Union Agency for Law Enforcement Cooperation, in April 2020.

Europol has been actively involved in the investigations led by France and the Netherlands since 2018, relating to the provision and use of encrypted communication services by organised crime groups. Through its role as an information hub and its extensive analytical and technical support system, Europol was able to create and provide a unique and global insight on the scale and functioning of organised crime, as a result of this investigation. This will help law enforcement to combat organised crime in the future more successfully. Europol's support from the early stages of this JIT included: promoting and arranging international cooperation, providing extensive analytical and financial support, technical expertise and a secured platform for the exchange of information between the countries involved. A large dedicated team at Europol investigated in real time millions of messages and data that it received from the JIT partners during the investigation, cross-checked and analysed the data, and provided and coordinated with the JIT partners the information exchange to concerned countries.

A large number of suspects have also been arrested in several countries which were not participating in the JIT but particularly affected by the illegal use of these phones by individuals active in organised crime, including in the UK, Sweden and Norway. Many of these investigations were connected with international drug trafficking and violent criminal activities.

At the same time, numerous operational meetings for the daily coordination between the law enforcement entities of the JIT partners and other countries took place at Europol, partly during COVID-19.

Eurojust intensively facilitated the judicial cooperation, during the extensive use of European judicial cooperation instruments such as European Investigation Orders. Throughout the investigation, the JIT members organised five coordination meetings at Eurojust to bring all involved parties together in a secure environment, identify parallel or linked investigations, decide on the most suitable framework for cooperation and solve potential conflicts of jurisdiction.

In France, where the operation takes place under the code name "Emma 95", the Gendarmerie has set-up a Taskforce since March 2020. With more than 60 officers, the Gendarmerie leads the investigations targeting the EncroChat encrypted telephone solution under the supervision of the magistrates of the JIRS of Lille. The Taskforce has been monitoring the communications of thousands of criminals, leading to the opening of a wide range of incidental proceedings. France does not wish to communicate further on these on-going investigations nor on the results obtained. The considerable resources deployed demonstrate the importance of these investigations and the importance attached to their success in France.

In the Netherlands, where the operation went under the code name "Lemont", hundreds of investigators have, with authorisation of the examining magistrate, followed the communications of thousands of criminals day and night since the operation began to unravel and act on the intercepted data stream. The criminal investigation has been led by prosecutors from the Dutch National Public Prosecution Service and the information has been made available to about a hundred ongoing criminal investigations. The investigation has so far led to the arrest of more than 100 suspects, the seizure of drugs (more than 8 000 kilo cocaine and 1 200 kilo crystal meth), the dismantling of 19 synthetic drugs labs, the seizure of dozens of (automatic) fire weapons, expensive watches and 25 cars, including vehicles with hidden compartments, and almost EUR 20 million in cash. The expectation is that

information will be made available in more than 300 investigations. In a number of cases, more arrests are very likely to follow in the coming period.

The interception of EncroChat messages came to an end on 13 June 2020, when the company realised that a public authority had penetrated the platform. EncroChat then sent a warning to all its users with the advice to immediately throw away the phones.

While the activities on EncroChat have been stopped, this complex operation shows the global scope of serious and organised crime and the connectivity of criminal networks who use advanced technologies to cooperate on a national and international level. The effects of the operation will continue to echo in criminal circles for many years to come, as the information has been provided to hundreds of ongoing investigations and, at the same time, is triggering a very large number of new criminal investigations of organised crime across the European continent and beyond.

WHAT IS ENCROCHAT?

EncroChat phones were presented to customers as guaranteeing perfect anonymity (no device or SIM card association on the customer's account, acquisition under conditions guaranteeing the absence of traceability) and perfect discretion both of the encrypted interface (dual operating system, the encrypted interface being hidden so as not to be detectable) and the terminal itself (removal of the camera, microphone, GPS and USB port). It also had functions intended to ensure the 'impunity' of users (automatic deletion of messages on the terminals of their recipients, specific PIN code intended for the immediate deletion of all data on the device, deletion of all data in the event of consecutive entries of a wrong password), functions that apparently were specially developed to make it possible to quickly erase compromising messages, for example at the time of arrest by the police. In addition, the device could be erased from a distance by the reseller/helpdesk.

EncroChat sold the cryptotelephones (at a cost of around EUR 1 000 each) at international scale and offered subscriptions with a worldwide coverage, at a cost of 1 500 EUR for a six-month period, with 24/7 support.

EMPACT

CRIME AREAS

Drug Trafficking • Cybercrime • Economic Crime

TARGET GROUPS

General Public • Law Enforcement • Academia • Professor • Students • Researcher • Press/Journalists • Other

COUNTRIES

France • Netherlands

ORGANISATIONS

Eurojust

SUPPORT & SERVICES

Operational coordination • Operational support • Information exchange • Analysis • Intelligence