Three years on, EncroChat cryptophone hack nets 6,500 arrests and seizures of €900m

Bill Goodwin ⋮ 12-15 minutes ⋮ 6/27/2023

An operation by French and Dutch police to hack EncroChat, an encrypted phone network used by organised criminals, has led to more than 6,500 arrests worldwide and the seizure of nearly €900m following three years of investigation.

Investigators intercepted, analysed and shared over 115 million supposedly encrypted text messages and photographs sent by users of EncroChat, with police forces in multiple countries disrupting organised drug gangs across Europe.

The operation led to the discovery of organised crime groups offering “crime as a service”, including kidnapping, extortion, assassination and in some cases torture, prosecutors revealed at a press conference today.

It has led to the seizure of more than 100 tonnes of cocaine, 160 tonnes of cannabis, three tonnes of heroin, and the seizure of over 900 weapons and more than 21,000 rounds of ammunition.

Europol worked with partner countries to identify messages that indicated a threat to life (TTL), which were provided as a live feed to law enforcement, including the UK’s National Crime Agency (NCA). The operation identified threats against at least one judge in an unnamed country.

The penetration EncroChat was a “game-changer”, said the deputy executive director of Europol, Jean-Philippe Lecouffe, and had boosted international cooperation in the fight against organised crime, leading to three further international criminal investigations.

Christophe Husson, second in command of the Gendarmerie’s cyberspace division, said the technical solutions developed for EncroChat would be used in other operations, including the exchange of crypto coins. “There are some investigations in progress as we speak,” he said.

Eurojust national member for France Baudoin Thouvenot said that the operation to infiltrate EncroChat, which had over 60,000 users, provided police with an up-to-date map of high-level organised crime, and had helped French government ministers to reflect the reality of drug trafficking in French ports.

Prosecutors used the press conference to criticise what they described as the circulation of “inaccurate and incomplete” information in the international press and on social media about the legality of the hacking operation against EncroChat.

Chief prosecutor at the judicial tribunal in Lille, which oversaw the EncroChat investigation, Carole Etienne, said the French investigation “was conducted in accordance with the applicable legal rules using a special investigative technique implemented in accordance with the provisions of the Code of Criminal Procedure”.

How French police hacked EncroChat

The French National Gendarmerie began investigating EncroChat in 2017 after recovering EncroChat phones from organised criminal groups involved in illegal drug trafficking. Subsequent investigations led to the discovery of EncroChat servers hosted at a datacentre run by cloud company OVH in Roubaix, France.

EncroChat sold its Android BQ Aquaris X2 and X3 Android cryptophones for around €1,000 each and offered subscriptions with worldwide coverage, at a cost of €1,500 for a six-month contract.

The phone promised users secure encrypted communications and anonymity by allocating a handle. It had the capability to delete messages and a PIN code to wipe the phone in case of an emergency.

Investigators were able to reverse-engineer EncroChat’s network of virtual machines used to manage encryption keys, analyse event logs, monitor the use of SIM cards, and to assign them to the right device, configure new phones and manage voice calls, customer services and other tasks.

The French internal intelligence agency DGSI (Direction Générale de la Sécurité Intérieure) supplied a software implant, delivered to phones disguised as a software update, which initially harvested historic data from the memory of infected phones, including stored chat messages, address books, notes and each phone’s unique IMEI number.

In stage two, the implant intercepted incoming and outgoing chat messages and transmitted them to a server run by the Gendarmerie’s Center for the Fight against Digital Crime (C3N) in Pontoise, in both stages using a compromised “load balancer” server at the Roubaix datacentre.

Separately, the UK’s NCA developed its own implant to penetrate EncroChat, which exploited an error logging software in the Android phone operating system,

known as the Marvin APK, to gather data, but chose not to deploy it after the French developed their own implant.

Dutch investigation

The Dutch National Police and public prosecutors office began an investigation, codenamed 26 Lamont, into the people running EncroChat, which was then one of the largest encrypted phone networks, in the Netherlands.

The Dutch set up a Joint Investigation Team (JIT) with the French in April 2020, with the support of the EU agency for diplomatic cooperation in the Hague, Eurojust, and the European Agency for law enforcement cooperation, Europol.

Dutch police analysed more than 20 million chat messages, which led to numerous investigations, arrests and convictions in the Netherlands, said Dutch national prosecutor for international cooperation Renske Mackor.

“We consider these suspects as important persons in the middle layer of the criminal organisation around EncroChat. They are related to the board of EncroChat and communicate with the layer of resellers,” she said.

Dutch police arrested three suspects in the Netherlands in 2022, under suspicion of participation in a criminal organisation, money laundering and complicity with crimes committed by EncroChat’s customers.

The suspects were initially held in pre-trial detention, but have been conditionally released. Mackor said she hoped a trial would take place in 2024.

A fourth suspect is on the run and being hunted by French and Dutch police.

French arrests

At its height in 2020, 100 gendarmes worked full-time on the EncroChat investigation centrally and in local offices in France. Ten gendarmes were deployed at Europol for 18 months.

French investigators have identified about a dozen people suspected of running EncroChat or being part of the EncroChat phone reseller network.

They include the main director of EncroChat, solutions developers, logistics managers, members of the money laundering structure and telephone resellers.

“The investigations into the EncroChat structure were complex, given the structure of the organisation itself, but above all given its location on various

continents, and required numerous acts of international corporation, some of which are still being prepared and/or implemented," said Etienne.

Crimes under investigation include the illegal supply, transfer and import of cryptographic devices in France, which incorporate offences committed in Canada, the Dominican Republic, Spain, the Netherlands, the UK, Germany, Hong Kong and Panama.

Three people were arrested in Spain in June 2022 and extradited to France under European arrest warrants. They have been charged with the association of criminals with a view to preparing crimes punishable with up to 10 years imprisonment, conspiracy to acquire, process or sell narcotics, conspiracy to import narcotics in an organised gang, aiding and abetting the acquisition of weapons and munitions, and money laundering.

Other people outside the European Union wanted in France have not yet been charged.

Some 84 further legal procedures are underway in France, including eight in Lille, described as "incidental" to the French investigation into owners and organisers of EncroChat.

They have led to 165 arrests and a seizure of over two tonnes of cannabis, in addition to 118 kilos of cocaine, 155 kilos of heroin, five weapons, 110 vehicles and over €4m in France.

Operation Emma

Europol set up an Operational Task Force (OTF), codenamed Emma, to analyse data gathered from EncroChat operating from its headquarters in the Hague.

Emma brought together investigators and experts from Europol, EU member states and other countries, including the UK, to assess the data.

A large, dedicated team of experts at Europol analysed over 115 million messages and data it received from the French and Dutch JIT partners.

Second in command of the gendarmerie's cyberspace division Christophe Husson said there were two major challenges – intercepting communications and then exploiting the mass of data collected.

Europol cross-checked and analysed 1.3TB (terabytes) of data, combining it with information in its own database to provide nearly 700 intelligence packages of data to countries worldwide. The investigation reached 123 countries.

“A joint investigation into EncroChat allowed us to discover a unique snapshot of organised crime and organised criminal groups that were that operating in the EU but also beyond,” said deputy executive director of Europol operations Jean-Philippe Lecouffe.

Lecouffe said Operation Emma multiplied the efforts made by the collaborating member states against organised crime and would be a model for future collaborations. Europol has since been supporting spin-off investigations initiated across the world, he said.

European courts say EncroChat is lawful

Prosecutors criticised reports that suggested the novel hacking operation might not be legal under European laws, pointing to court decisions in The Netherlands and France that found evidence from the hacked phone network could be used in criminal cases.

The Dutch Supreme Court ruled on 13 June 2023 that Dutch courts could lawfully use material gathered by French investigators from EncroChat and a second encrypted phone network, Sky ECC, in evidence in Dutch criminal cases.

The court found, following referrals by two regional courts in the Netherlands, that Dutch courts should respect judicial decisions underpinning investigations in other countries in criminal cases, citing the principle of “interstate trust” between EU member states.

This would continue to be the case unless a court in the collaborating country irrevocably ruled that the investigation was unlawful or there were concrete indications that the results of the investigation may not be trusted, said Mackor.

The Netherlands Forensic Institute (NFI) examined the reliability of the results of the French interception tool and reported that they see no reason to doubt the reliability or trustworthiness of the data it gathered, she added.

“The Supreme Court has furthermore ruled that in the present criminal cases, concrete indications that the data would not be trustful are lacking. Thus, for now, the Dutch Prosecution Service sees no need to review the reliability of the data,” she said.

The ruling by the Netherlands Supreme Court fits in with other rulings in European courts concerning the assessment and use of evidence derived from the French investigations into EncroChat and Sky ECC.

“It marks an important trend in the admissibility and reliability of evidence from data sourced from the French investigation. In that aspect, it also marks a new

period in international jurisprudence," she said.

"The expectation is that in future cases related to organised crime, the sharing of evidence and cooperation in obtaining evidence will become even more crucial."

French Supreme Court ruling

The criminal division of the French Supreme Court, the Cour de Cassation in Paris, has issued two rulings on the validity of the EncroChat data capture.

Carole Etienne, chief prosecutor at the judicial tribunal in Lille, said the first ruling on 11 October 2022 validated the capture and modification of any computer system under French law, and acknowledged the use of national defence secrecy to protect the operation of the capture device complied with the French constitution.

In the second ruling, on 10 May 2023, the court confirmed that given the absence of data and description as part of the digital capture process, French investigators were not required to produce a certificate of truthfulness to authenticate the data used in prosecutions.

In the UK, the Investigatory Powers Tribunal ruled in May 2023 that the NCA lawfully obtained warrants to receive messages from the hacked EncroChat phones. The admissibility of EncroChat evidence continues to face legal challenges in a number of crown courts.