Inside the Met Police's investigation into EncroChat crime gangs - Blog - Creative Collaboration

10-12 minutes ⋮ 1/8/2024

It was in the midst of the Covid pandemic in spring 2020 that DCI Driss Hayoukane, a senior investigating officer at the Metropolitan Police, was let into an extraordinary secret.

Summoned by his boss to a highly confidential meeting, Hayoukane learned that French police had worked out how to eavesdrop on a telephone network used by the world's most dangerous organised crime groups.

Having spent 30 years investigating organised criminals, Hayoukane had planned to spend his retirement following another passion – training and coaching young people in football. But what he heard at the meeting changed all that.

With his retirement plans now on hold, the DCI was asked to assemble a team at short notice to prepare to analyse whatever the French could provide.

Working from a huge secure building somewhere in London, "with all the technical wizardry" the police and other investigative agencies could muster, the Met's team found itself with direct access to the communications of London's criminal gangs.

"We could not cope with the amount of data we were getting. We were overwhelmed," Hayoukane told the BBC in a podcast series released this week. "It was just like cracking open a window straight into an organised crime group."

For over two months from April 2020, Met officers were able to eavesdrop on messages sent by 1,400 suspected criminals who were unaware that their supposedly secure EncroChat encrypted phones had been compromised by a French hacking operation.

It was, according to the six-part BBC podcast, *Catching the Kingpins*, the biggest organised crime bust in British policing history, leading the Met Police to arrest 950 suspected criminals and secure convictions against 750 of the most dangerous criminals.

The Met's operation against EncroChat, codenamed Operation Eternal, uncovered corrupt police officers in the pay of organised crime, murder conspiracies, an illicit trade in fire arms and drugs, and for the first time gave the Met police a detailed picture of the links between rival crime groups.

Hayoukane first began noticing that many suspected drug traffickers were using EncroChat phones in 2017. EncroChat handsets – which are essentially modified Android phones with sophisticated encryption built in – were designed, he said, for "criminal use".

The phones were expensive, typically costing £1,500 for the handset and £1,500 a month for a subscription. They were sold through a network of resellers, who would meet buyers in person, under the counter in some phone shops, or over the web for bitcoin. Each phone came with a "duress PIN", which once entered would irretrievably wipe the contents of the phone.

The mystery behind EncroChat

The people behind EncroChat is still a matter of speculation. EncroChat was registered in Panama in 2014 and another company of the same name in Hong Kong in 2013.

What is known is that the phones were sold initially from Canada by a company that specialised in selling phones to legitimate users who were interested in protecting their privacy.

Geoff Green, its principal, met with representatives of EncroChat, then known as EsoCrypt, over dinner in 2014 and was sufficiently impressed to agree to resell the phones, which at that stage were built around off-the-record (OTR) encrypted messaging.

Green wrote in a blog post that his relationship with EsoCrypt turned sour in 2016 after learning that the company had been sold to a new, anonymous owner. The new owner, he wrote, abruptly ended the business relationship with Green, costing him millions in lost revenues.

In 2022, a French newspaper reported that the purported CEO of EncroChat had been arrested in the Dominican Republic, while France extradited three people alleged to have been involved in reselling EncroChat phones from Spain.

> *The Metropolitan Police arrested 950 suspected criminals after obtaining hacked data from EncroChat encrypted phones*

The evidence in the data

By the time EncroChat phones began to attract the interest of police in the UK, EncroChat was offering its customers encrypted messaging services and secure note taking, using encryption based on Signal – the same type of encryption used by WhatsApp and other services.

EncroChat users used anonymous handles, with names like "Usualwolf" and "Nudetraine", but French computer crime investigators were able to identify phone users operating from the UK by linking the handles to Wi-Fi networks and cell towers accessed by the phones.

In the UK, data scientists created computer scripts to analyse incoming messages from the French to help Met Police investigators prioritise their time. "We were looking for key words, such as murder, armed robbery, kidnap, firearms, child sexual exploitation, modern slavery, high-level drug importation, corruption, threats to life," Hayoukane told the BBC.

Keeping the EncroChat secret

The police went to great lengths to ensure that news of the EncroChat hacking operation did not leak to organised crime groups. For example, police found other reasons to arrest EncroChat suspects, and in some cases, criminals were allowed to go free to preserve the secret.

In spring 2020, according to defence lawyer Julian Richards who was interviewed by the BBC, there was an unexplained surge of arrests and drug seizures. The police seemed to have inside information, but where it came from was anyone's guess, creating more buzz on EncroChat as criminal groups started speculating whether their co-workers or colleagues were passing information to the police.

The Met's analysis showed that EncroChat and similar cryptophone networks had changed the nature of organised crime. Where once members of the most dangerous drug gangs would have served a 20-year apprenticeship, now anyone with money could buy an EncroChat phone and set themselves up as a dealer. It was a badge of credibility.

The criminals who gave themselves away

Investigators were astonished by the careless way suspects gave away their identities in EncroChat messages, perhaps lulled by a false belief in the impregnability of the phone's encryption. In one case, a suspect sent a text message giving their name, date of birth and address. In other cases, suspects blatantly exchanged selfies.

“The communication wasn’t always strictly business. There was a kind of chit-chat as well, and a lot of times you can pick up little clues,” said Hayoukane.

For example, Paul Fontaine, who was convicted of conspiracy to murder, gave himself away by taking his EncroChat phone along with his ordinary registered mobile phone on journeys from London to Cardiff. Both phones connected to the same cell towers at the same time, making it highly likely that Fontaine was the owner of the EncroChat phone.

Fontaine’s client, Frankie Sinclair, who had asked Fontaine to find him a gun, was even more careless. He sent Fontaine a photograph of his mum’s house, showing his mum’s car and her registration plate. Sinclair was later convicted of murder.

Harry Hicks-Samuels, a cocaine trafficker, was caught after he boasted to his contacts on EncroChat about ordering a takeaway from an expensive restaurant in Mayfair and joining an upmarket golf club, effectively handing the police two shortlists of suspects. Hicks-Samuels was the only name on both lists.

In another example of criminal hubris, money launderer Lee Hannigan boasted about the model of his Ferrari and mentioned he had missed his MOT, handing police clues that led to his identity being discovered.

Business trumped gang rivalry

Analysis of the phone metadata has enabled the Metropolitan Police to build up a network diagram showing the links between different criminal groups, creating what is, in effect, a map of the criminal underworld.

The map has helped to overturn previous assumptions about gang rivalry. There may be conflicts between different groups of criminals, but that does not prevent them talking to each other. “Business trumps everything … everyone’s really talking to everyone else,” said Hayoukane.

Before the hacking operation, the Met did not know whether organised crime groups involved in drug smuggling were also involved in human trafficking. The Met’s network diagram reveals this is not the case. Although human trafficking gangs did use EncroChat phones, they were far outnumbered by drug gangs, and there was little communication between the two groups. The Met found no evidence of terrorist gangs or paedophiles using EncroChat.

The data shows that many organised crime suspects had links with Dubai and the United Arab Emirates. They include Kashif Mahmoud, a corrupt former Metropolitan police officer who took part in heists staged by organised crime gangs on rival groups orchestrated from Dubai.

The country has replaced Marbella as the destination of choice for organised crime, said Hayoukane. "It's got sunshine, people speak English, its easy to get to and it's the hub to the world." Another reason may be that extradition from Dubai to the UK is not always straightforward.

According to the National Crime Agency (NCA), working with the Regional Organised Crime Units, HMRC, and other government agencies, police across the UK have arrested over 3,000 people, leading to 1,000 convictions. Police have seized 173 firearms and 1,000 rounds of ammunition. Add to this three tonnes of heroine, 14.5 tonnes of cannabis and £80m in seized cash, and the operation has clearly had a major impact on drug dealing and money laundering gangs.

Yet figures quoted by the BBC show that three years on from the EncroChat operation, there has been no measurable reduction in the use of illegal drugs in the UK. When the police take out one kingpin, another steps in to take their place.

For Wayne Johns, a senior investigating officer at the NCA, it's important to look at the bigger picture.

"If you've taken those weapons off the street, if you've taken that money off these individuals and, to be honest, if you've taken those drugs out of circulation, that's six tonnes of drugs that aren't on the street and aren't impacting communities," he said.

Gangster Presents: Catching the Kingpins is available on BBC Sounds.