

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.

<https://www.wsj.com/articles/massive-hack-gave-police-a-window-on-cocaine-cash-and-killers-11637680356>

EUROPE

Massive Hack Gave Police a Window on Cocaine, Cash and Killers

Criminals thought encrypted Sky ECC cellphones were impregnable, but cops tapped a billion messages, yielding arrests and drug seizures

By [James Marson](#)

Nov. 23, 2021 10:12 am ET

BRUSSELS—The gangsters plotting to assassinate a judge thought they were leaving nothing to chance. But cops hundreds of miles away were on to them thanks to a stakeout with a modern twist.

Using supposedly impregnable encrypted phones, the Serbian hit men discussed earlier this year how wind direction and distance could affect the sniper's bullet and planned their getaway. Unbeknown to them, their messages were also flashing up on the computer screens of a secret police team in Belgium that had hacked into the messenger service, called Sky ECC. The Belgians warned police in Serbia, who whisked the judge to safety.

The infiltration was a signature success in efforts by authorities across the world to counter encrypted communications—a powerful new tool for criminal gangs to hide their identities and hatch plans in secret.

Special handsets with a secure chat app and most other functions disabled have helped criminals flood Europe with cocaine, turning it into a rival of the U.S. for the world's biggest market, according to the U.S. Drug Enforcement Administration.

But when authorities got inside the networks, they gained an unobstructed view of the gangs at work—and the chance to thwart them. For three weeks in February and March, Belgian officials say they eavesdropped as criminals used Sky to coordinate massive drug shipments, plan hits and exchange photos of cash, cocaine and corpses.

“It’s their Achilles’ heel,” said Kevin Daniels, the DEA’s deputy chief for Europe.

“Oftentimes we’re two or three steps behind. They are looking for the latest technological advantage over us. But we’re finding a way to catch up.”



Andy Kraag, chief of the Dutch National Criminal Investigation Department. Around one-quarter of active Sky users were in Belgium and the Netherlands, according to prosecutors.

PHOTO: EVERT ELZINGA/AGENCE FRANCE-PRESSE/GETTY IMAGES

Law-enforcement officials say infiltrating Sky was the largest of several recent strikes against encrypted platforms. Authorities gathered roughly one billion messages from tens of thousands of Sky-enabled devices world-wide, which could feed investigations for years. Belgium has detained more than 500 suspects and seized 88 metric tons of cocaine, already exceeding last year's record haul.

“Sky was monstrous,” said Scott A. Albrecht, who served as the DEA's attaché in Belgium until July. “It was so global and such a volume of messages.”

This account of the international operation against Sky is based on interviews with a half-dozen officials from Belgium and the DEA, as well as public accounts from U.S., Belgian and other European officials. The company that owned Sky, Vancouver-based Sky Global Inc., has denied any wrongdoing and said the platform had the legitimate aim of protecting privacy, not facilitating criminals. Sky Global says it relied in many cases on third-party resellers to distribute its devices and sought to prevent them from supplying criminals.



A haul of cocaine was seized in Brazil in August. The aircraft was bound for Brussels, according to Brazilian police.

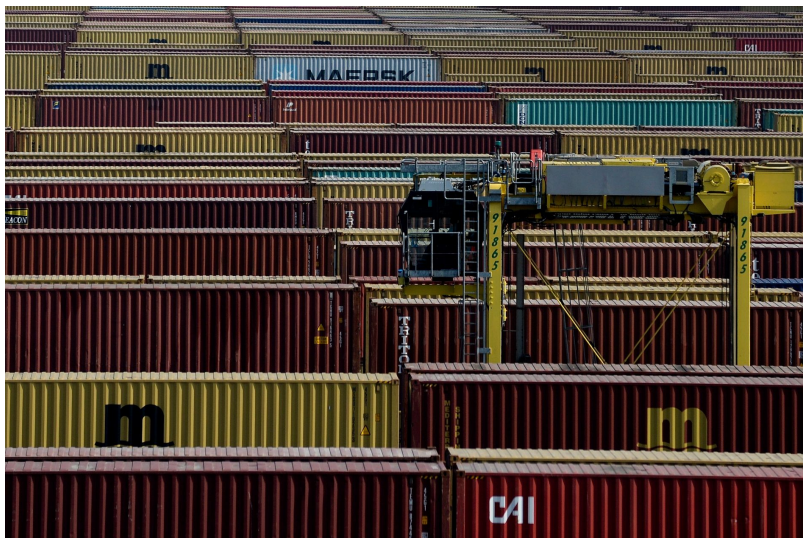
PHOTO: BRAZILIAN FEDERAL POLICE/AGENCE FRANCE-PRESSE/GETTY IMAGES

It was 2018 when Belgian police began picking up cellphone handsets that they couldn't read. But when authorities mapped where similar phones were connecting to transmission towers, they found locations that were familiar from their efforts to counter the torrent of cocaine entering Europe via ports like Antwerp.

Sky, through its website and a network of resellers, offered Apple, Google and BlackBerry handsets loaded with sophisticated encryption software and with their GPS, cameras and microphones disabled. Messages were automatically deleted after 48 hours if the contact wasn't reachable, and devices could be wiped remotely. Sky billed the platform as impenetrable and offered a prize of up to \$5 million to anyone who could hack it.

Sky had tens of thousands of active users from the U.S. to Colombia to the Middle East. According to Belgian prosecutors, around one-quarter were in Belgium and the Netherlands, two of the main gateways to Europe for cocaine.

Sky said its target market was people and entities concerned with data privacy and confidentiality, such as doctors, government contractors and celebrities. But the locator map appeared to confirm that the phones, with contracts costing as much as \$2,500 for six months, were being used almost exclusively by criminals.



The torrent of cocaine entering Europe via ports like Antwerp has turned it into a rival of the U.S. for the world's biggest market.

PHOTO: JOHANNA GERON, PRESS POOL

Authorities needed to establish whether it was a legitimate target for infiltration, so they turned to traditional sleuthing methods. When a phone connected to a tower, revealing its location, they would use security cameras and dispatch surveillance teams to identify the users. Many of them turned out to be people suspected of involvement in drug-related crimes.

Authorities tracked a Sky server to northern France and worked with officials there to gain access. At first, they could only see the metadata, including the nicknames of users and the names of group chats, but not the messages. Then, an international team of hackers from as far afield as Australia found a way to decrypt roughly half of the three million daily messages.

“That was the Holy Grail,” said Belgian Justice Minister Vincent Van Quickenborne.

Authorities launched a live operation in mid-February, reading messages in near-real-time and seeking to thwart criminals or catch them red-handed. Dozens of Belgian police across two sites in Brussels and Antwerp, along with teams in France and the Netherlands, tracked the conversations of top targets and received messages from others filtered for keywords by artificial intelligence.



The price of a kilo of cocaine rises significantly when it lands in Europe.

PHOTO: FEDERAL JUDICIAL POLICE ANTWERP/ASSOCIATED PRESS

The messages and photos pinging across the world astounded even experienced investigators. Users, confident in the platform's impregnability, shared pictures of corpses, severed heads and other body parts, as well as bricks of cocaine and stacks of cash. One user sent a photograph to demonstrate he had carried out an order to torture a victim. When one enforcer in a Western European country couldn't find the man he was supposed to pummel, he received new instructions: "Here are pictures of the wife. You can break her legs."

The messages revealed new connections and methods, from Belgian links with Italian organized crime to laboratories used by Colombians to extract cocaine hidden in fruit juice or melted into the plastic of toy dolls.

"Normally in an investigation, you have to dig a lot to find a small piece of gold," said Belgian Federal Prosecutor Frédéric Van Leeuw. "Here, we had an open gold mine."

The teams had to decide whether to act on the information, given the risk of exposing the operation, but always did so in case of threats to life. In one case, a message indicated that a gang in Canada was about to begin torturing a captive. The Belgians called authorities there to intervene.

Police also used information about shipments to seize tons of cocaine, although the big targets would sometimes shrug off the losses as they were making so much money. A kilo of cocaine costs €4,000 in Colombia, the equivalent of around \$4,500, but rises to €50,000 in Belgium, where it is cut, increasing profits.

"They said, 'Forget about it,'" said Mr. Van Leeuw.

After police seized a large consignment at the port in Antwerp, one group exchanged messages blaming a partner for snitching and proposing to kill him. Authorities decided to end the operation instead of risking an outbreak of violence.

On March 9, 1,600 Belgian police officers carried out more than 200 searches across the country, detaining 48 suspects.



An employee at the port of Antwerp shows an X-ray scan of a truck carrying a shipment of cocaine.

PHOTO: ARIS OIKONOMOU/AGENCE FRANCE-PRESSE/GETTY IMAGES

Three days later, the U.S. Department of Justice said that a federal grand jury in San Diego had indicted the chief executive of Sky Global and an associate on racketeering and drug-trafficking charges, saying the encrypted phones had facilitated the distribution of drugs. A court issued warrants for their arrest, and the U.S. government seized the company's websites, essentially forcing the shutdown of the encrypted service.

Lawyers for Sky Global filed a legal complaint this month in a federal court in San Diego, alleging that the U.S. government had improperly shut down Sky ECC and painted the executives as criminals for providing encrypted technology. The motion asked the government to return the company's web domains, saying that it had taken measures to prevent its use for illegal activity, such as cutting off unscrupulous resellers.

Since the busts in March, police in Belgium have identified nearly 2,500 suspects and detained hundreds more, from suspected gangsters to police commanders and employees from port terminals, shipping firms and security companies. Several hundred police officers are pursuing further investigations. The first trial using the intercepted messages is set to start in January.



Belgian police have detained dozens more suspects since March.

PHOTO: NICOLAS MAETERLINCK/BELGA/AGENCE FRANCE-PRESSE/GETTY IMAGES

Meanwhile, officials say criminals are adapting by communicating across several platforms, for example by sending the numbers of containers containing shipments of cocaine in two parts via different services. Others are using popular messengers like WhatsApp, seeking to hide among the deluge of communications over such platforms.

New platforms are also popping up.

“It’s like whack-a-mole,” said the DEA’s Mr. Albrecht. “You hit one on the head, and then there comes two more.”

Write to James Marson at james.marson@wsj.com

Appeared in the November 24, 2021, print edition as ‘Hack Revealed Cocaine, Cash and Corpses.’

Copyright © 2021 Dow Jones & Company, Inc. All Rights Reserved

This copy is for your personal, non-commercial use only. To order presentation-ready copies for distribution to your colleagues, clients or customers visit <https://www.djreprints.com>.