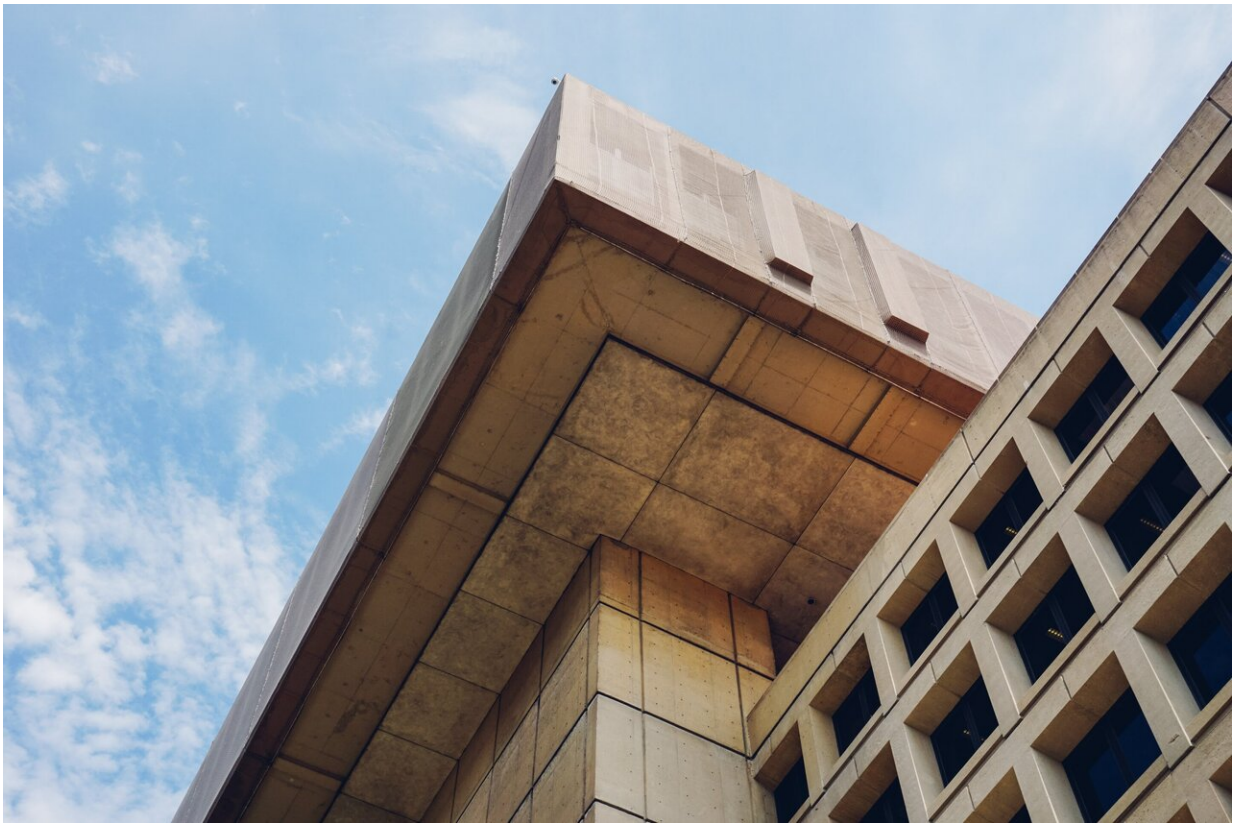
'What's the price today?': FBI phone app reaped secrets of global drug networks

June 8 2021



Credit: Unsplash/CC0 Public Domain

One drug trafficker texted another that he had a "job" and a proven way to get it done: two kilograms of cocaine from Bogota using the French embassy's protected diplomatic pouch.

The pair were straightforward, because they were using the newest, safest mode of communicating: a special-purpose, highly encrypted, messaging-only cellphone called ANOM that operated on a closed network.

"They have already got a few packages in," Baris Tukel told buyer Shane Geoffrey May, according to US court documents.

As proof, Turkel texted pictures of the pouch bound and stamped "Valise Diplomatique Francaise" and another shot of tightly wrapped drug packs.

"They can do it weekly," he wrote.

Little did they know that ANOM was produced and distributed by the US Federal Bureau of Investigation, and every one of their messages—and those of thousands of other criminals around the world—were being copied directly to an FBI server.

27 million messages

Others had the same sense of security. They bickered over prices, and explained smuggling strategies.

Using ANOM, "Ironman" texted "Real G" on how they could get volumes of cocaine into Hong Kong, where they had no one in customs to shepherd it through.

The answer? "Real G" sent "Ironman" a photograph of drug packages layered in between bananas in a shipping crate. First, he said, they would have to send some legitimate banana shipments to ease the way.

Their messages were some of 27 million that the FBI and law

enforcement partners in Australia and elsewhere scooped up and decrypted, exposing global criminal networks to an unparallelled extent.

The US Justice Department said "Operation Trojan" Shield reaped a "staggering" amount of intelligence that has led to 800 arrests.

It turned one of the biggest challenges for law enforcement today, widely available, unbreakable encryption apps on cellphones, to law enforcement's advantage.

Officials on three continents announced Tuesday that they had seized 38 tons of cocaine, marijuana, methamphetamine and precursor chemicals; 250 firearms and currencies worth $48 million in the operation.

Some 50 clandestine drug labs were shut down and more than 100 potential murders disrupted.

Law enforcement officials themselves seemed in awe at the result of "Trojan Shield".

FBI Special Agent Suzanne Turner said they were stunned at how openly traffickers exchanged information on the ANOM devices.

"They believed it was secure communications," she told reporters in Washington.

FBI had master decryption key

The massive coup came about in 2018, when the FBI shut down a precursor encrypted service called Phantom Secure and arrested its head Vincent Ramos and four others for supporting drug trafficking.

That appears to have led the FBI to a builder of the phones who was

working on the next generation. The tech wizard already had one drug conviction and faced new charges.

So they agreed to produce ANOM for the FBI, who paid him or her $170,000 to do so—adding to the encryption system a digital master key that only the FBI could use.

ANOM would also copy all messages from a user to an FBI-controlled server located in a third country as they were transmitted.

But how to get the bad guys to buy the phones, at $2,000 apiece?

The builder already had a network of trusted distributors in place from previous products, and pitched ANOM to them with the pitchline, "Enforce your right to privacy."

The phone hit the market in October 2018, with distributors first selling about 50 in Australia for a Trojan Shield beta test, the FBI working with the Australia Federal Police.

By 2019 ANOM devices were found around the world, used the most in Germany, Netherlands, Spain, Australia and Serbia, mainly by drug traffickers and money launderers.

The FBI said more than 300 distinct transnational criminal organizations were using ANOM.

Shutting down rivals

It had its competitors. The FBI discovered that some gangs compartmentalized operations by different communications technology.

In one, ANOM was used for the logistics of the drug shipments, while

Ciphr or Sky were used to deal with the money involved.

But ANOM gained in popularity as law enforcement went after other devices, like in 2020 when European authorities brought down up EncroChat, a four-year-old encrypted handset.

After US authorities closed down another rival, Sky Global, in March this year, active ANOM users soared from 3,000 to 9,000, the FBI said.

Why was ANOM shut down now? Turner said Tuesday that many legal cases were ripening and that "it was time to get these criminals off the street."

But a March blog post by an unknown writer claiming that ANOM was transferring data to unknown servers may have also threatened to expose the network.

Citation: 'What's the price today?': FBI phone app reaped secrets of global drug networks (2021, June 8) retrieved 10 April 2024 from https://techxplore.com/news/2021-06-price-today-fbi-app-reaped.html