ANOM global phone sting: What we know

June 8 2021

Credit: CC0 Public Domain

Law enforcement agencies from three continents on Tuesday revealed a vast FBI-led sting operation that sold thousands of supposedly encrypted mobile phones to criminal organisations and intercepted their messages for years.

Police accounts and unsealed US court documents, first cited by Vice

News, reveal an ambitious worldwide plot that was years in the making.

What is ANOM?

ANOM was billed as a fully secure encrypted mobile phone that promised the user total secrecy in communications.

Essentially it was a jailbroken handset that used a modified operating system—removing any of the normal text, phone or GPS services that would make it trackable and traceable.

On the surface, the device would look like a normal mobile phone, but it contained a "secure" messaging service hidden behind a functioning calculator app.

In theory, the phone operated on a closed network—ANOM phones could only communicate with other ANOM phones using "military grade" encryption that transferred data via secure proxy servers.

The phones also contained a kill switch to delete contacts or any other data stored locally.

Similar services like Phantom Secure, Sky Global, Ciphr, and EncroChat have for years been used by criminal networks for planning and communication—and many have been exploited by law enforcement.

Where did the FBI come in?

In March 2018 Phantom Secure's CEO Vincent Ramos was indicted by grand jury and along with colleagues would eventually plead guilty to a raft of charges related to drug trafficking.

Shortly after that, an unnamed "confidential human source" presented

the FBI with a next-generation encrypted device—that would be dubbed ANOM—which was designed to replace discredited, defunct or infiltrated systems.

The same source agreed to disseminate the now FBI-compromised devices among a network of blackmarket distributors who had sold Phantom Secure to carefully vetted or vouched-for individuals, usually members of organised criminal gangs.

Why did criminals buy it?

Initially, 50 ANOM phones were distributed in a test run, mostly to members of Australian organised criminal gangs.

But through word of mouth they gained in popularity with criminal underworld figures, who reportedly recommended them to friends.

Interest in ANOM exploded in 2020 when European authorities rolled up EncroChat, with dozens arrested, and after Sky Global CEO Jean Francois Eap was detained.

In the end, the FBI, Australian authorities and an unnamed "third country" were able to access more than 20 million messages from 11,800 devices in 90 countries.

They were most popular in Germany, the Netherlands, Spain, Australia and Serbia.

Why did the operation stop?

There is no clear rationale given about why the operation stopped now. However a mixture of suspicions, legal hurdles and strategy may have contributed.

Law enforcement did not have real-time access to phone activity but instead, all sent messages were blind copied or 'BCCed' to FBI servers where they were decrypted.

One server was in a third country where the warrant was due to expire on June 7, 2021.

But even ahead of that deadline, suspicions were being raised.

In March "canyouguess67" posted on WordPress that ANOM was a "scam" and that a device he had tested was "in constant contact with" Google servers and relayed data to non-secure servers in Australia and the United States.

"I was quite concerned to see the amount of IP addresses relating to many corporations within the 5 eyes Governments (Australia, U.S., Canada, UK, NZ who share information with one another)," the post said before it was deleted.

In addition, one stated aim for "Operation Trojan Shield" was to undermine trust in encrypted devices, a goal that could only be widely achieved when the operation was made public.