‘We Have to Run a Good Company’: How the FBI Sold Its Encryption Honeypot

The FBI had to run its Anom encrypted phone company just like any other, a former Department of Justice official who worked on the case told Motherboard.

By Joseph Cox

09 June 2021, 10:45pm

IMAGE: OLIVIER MORIN/AFP VIA GETTY IMAGES

The FBI had a problem. For years, serious organized criminals have been using encrypted phone companies such as Phantom Secure, Sky, and Ciphr to talk to their associates. These phones, which sometimes strip out GPS functionality and offer

but aren't perfect.

Last year, French authorities penetrated one of these services and were able to read millions of encrypted messages that led to hundreds of arrests across Europe. The FBI's plan was even more bold. Rather than penetrate an existing encrypted phone company used by criminals, it would secretly start and market its own encrypted phone firm. While criminals used the devices, the FBI would be able to read what they were saying.

The challenge was that running a fake encrypted phone company was not that different from running a real encrypted phone company.

"We can't just run a good investigation; we have to run a good company," Andrew Young, a partner in the Litigation Department in law firm Barnes & Thornburg's San Diego office and former Department of Justice lead prosecutor on the Anom case until he left in August 2020, told Motherboard in a phone call.

It was essentially a problem of marketing, Young said. The FBI needed to imbue this fake company with credibility so that criminals would buy and use the phones.

The FBI began working on the nuts and bolts of creating and running a company. It had to run customer service, solve technical problems for users, and potentially deal with hackers too, Young said. The FBI was entering an industry where firms hack or otherwise disrupt one another in an attempt either to discredit their rivals. Anom had to look like the new phone that criminals wanted to use.

Young said the FBI had to "figure out how we could develop a legal framework that protected the rights of the people whose rights we were obligated to protect, to develop admissible evidence against the criminals that were using it, to get an understanding of how, logistically, this would work, to establish what the bureaucratic obstacles would be and how to get it through our various agencies and governments to be approved, and essentially how to get it in the hands of criminals."

to the criminal underworld to start selling Anom, according to court records.

"We essentially copied what Phantom did; we copied what we saw other companies were doing," Young said. Eventually, the FBI was successful: this week law enforcement agencies in Australia, Europe, and the U.S. announced the operation, dubbed Trojan Shield, where Anom devices had obtained over 27 million messages from users in over 100 countries.

> ***Do you know anything else about Anom? Were you a user? Did you work for the company? We'd love to hear from you. Using a non-work phone or computer, you can contact Joseph Cox securely on Signal on +44 20 8133 5190, Wickr on josephcox, OTR chat on*** jfcox@jabber.ccc.de***, or email*** joseph.cox@vice.com**.**

The FBI had long wanted to get inside an encrypted phone firm. As Motherboard previously revealed, the FBI initially tried to get a backdoor into Phantom Secure, an encrypted phone firm popular across the world and used by bikers and the Sinaloa drug cartel. The FBI cornered the company's CEO Vincent Ramos in a Las Vegas hotel room, but Ramos declined to help. Shortly after, a confidential human source (CHS) who distributed Phantom phones offered the FBI access to Anom: "It became absolutely the plan to have the FBI establish a covert company," Young said.

As Motherboard reported on Monday, that started with a beta test of the idea in Australia, with authorities distributing around 50 devices to targets in the country.

The operation was extraordinarily complex, Young said. "How do you grow something on a worldwide level, and with cooperation with multiple countries, multiple governments, and not have it ever leak out?," he said.

The FBI also needed to avoid having the phone become mainstream, because if the devices ended up in the hands of the general public, that would bring up serious ethical and legal issues concerning surveillance of people not involved in the criminal underworld for a project that could already be seen as controversial.

Motherboard that Anom "went pretty hard" in the country. At the time, they wouldn't have known this was actually the FBI. Motherboard granted the distributor anonymity to speak more candidly about sensitive industry developments.

Initially, people used Anom as a secondary phone along Ciphr, another encrypted phone firm popular with criminals in Australia, the distributor explained. As one Anom court record said, during the operation law enforcement found that some criminals used one series of phones for discussing the logistical part of a drug shipment, and used another network such as Ciphr or Sky for talking about the concealment of illicit proceeds. Often, encrypted phone companies only let users speak to one another solely on their network, meaning users may need to have two different phones on different networks to speak to specific people.

"However within the last three months I have heard people talk about them [Anom phones] regularly, and the people I asked about them all knew what I was talking about," the former Phantom distributor told Motherboard.

Besides announcing the undercover operation this week, the Department of Justice also unsealed an indictment against 17 people for allegedly working for Anom.

Tech

The Network: How a Secretive Phone Company Helped the Crime World Go Dark

JOSEPH COX

10.22.20

Domenico Catanzariti, an Australian national, was allegedly an administrator for Anom and is charged in the indictment under the Racketeer Influenced and Corrupt Organizations Act. Administrators were tasked with setting up new subscriptions for customers, removing accounts, and remotely wiping devices that had been seized by law enforcement. Motherboard confirmed Catanzariti was a former notable distributor of Phantom devices in the country before joining Anom. As part of a multi-year investigation into Phantom, Motherboard obtained an FBI-authored document laying out the investigation concerning the company. One page of that 30 slide

the country they operated in. Catanzariti is listed as a distributor for South Australia in the document.

In one of the Anom court records, the FBI writes that Anom started by employing three unwitting former Phantom distributors to start selling Anom devices. These people, "seeing a huge payday," agreed to work for the company, the record says.

Other people who worked on Anom according to the indictment are spread across the world. Maximilian Rivkin, a Swedish national based in Turkey and who worked for Anom as an administrator and influencer, was expelled from Colombia in 2019 after what the government there said were a series of crimes at a hotel.

> **"We wanted to shatter the trust in the encrypted phone industry that catered to criminals."**

Baris Tukel, an Australian now based in Turkey accused of being an Anom distributor, has long running connections with Australia's bike gangs, according to the Guardian. Tukel is currently an international fugitive.

Hakan Ayik, a drug trafficker that Australian media dubbed The Facebook Gangster for his prolific social media posting, is allegedly responsible for introducing Anom devices to some criminal Australian users in the first place. Due to the threat to safety he may now face for unknowingly helping the FBI, Australian authorities are encouraging Ayik to turn himself in.

All of these people, although working for the same company, were anonymous even to each other, according to court records.

"Typically within this world, they try to stay as anonymous to each other as they can," Young said. "We had to recognize that from the outset; we can't ask people to

suspicious from their perspective.

So part of the task was not just uncovering crime and mitigating any serious threats to life that came up. The operation also involved identifying who was using these devices.

"That's true whether it's a wiretap of three people in Southeast Los Angeles, or 10,000 people throughout the world," Young said.

Typically when authorities shut down one encrypted phone company, its users flock to another firm, which may run special offers for new customers. At the moment, one of the more established remaining companies is Ciphr. It's unclear if Ciphr's user base has increased after the closure of Anom; Ciphr declined to comment on the Anom case in an email to Motherboard on Wednesday.

"We wanted to shatter the trust in the encrypted phone industry that catered to criminals," Young said.

"Whether that means they go back to hand-written notes and walking in the park, and covering their mouths so nobody can read their lips, or whether that means they go onto more legitimate mediums," he added. "What we try to do is at least take away this tool from them, because it was so clearly criminal."

Subscribe to our new cybersecurity podcast, CYBER.

TAGGED: WORLDNEWS, WORLD PRIVACY, ENCRYPTION, GOING DARK, PHANTOM SECURE, ANOM, SKY SECURE

MORE FROM VICE

Tech

Scammer Made Thousands Selling 'Leaked' Frank Ocean Tracks That Were Fake, AI-Generated

JOSEPH COX

05.10.23

Tech

Internal Emails Show FBI Freaking Out About Deepfakes

JOSEPH COX

07.07.23

Tech

FTC Orders Ring to Pay $5.8 Million in Refunds For Surveilling Customers, Failing to Stop Hackers

JOSEPH COX

05.31.23

Tech

People Are Pirating GPT-4 By Scraping Exposed API Keys

JOSEPH COX

06.07.23

Tech

'Windows for Gamers' Rolls Dice With Your Security

JOSEPH COX

Tech

The Car Thieves Using Tech Disguised Inside Old Nokia Phones and Bluetooth Speakers

JOSEPH COX

04.18.23