Trojan Shield: How the FBI Secretly Ran a Phone Network for Criminals

7-9 minutes

Hacking. Disinformation. Surveillance. CYBER is Motherboard's podcast and reporting on the dark underbelly of the internet.

For years the FBI has secretly run an encrypted communications app used by organized crime in order to surreptitiously collect its users' messages and monitor criminals' activity on a massive scale, according to a newly unsealed court document. In all, the elaborate operation netted more than 20 million messages from over 11,800 devices used by suspected criminals.

The news signals a major coup for law enforcement: ordinarily, agencies either shut down or crack messages on an already established service, such as Phantom Secure or Encrochat, two similar encrypted messaging networks. But in this case, the FBI took control of a communications company called Anom in its infancy and turned that into a wide-reaching honeypot, with the suspected criminal users instead coming to them.

"The FBI opened a new covert investigation, Operation Trojan Shield, which centered on exploiting Anom by inserting it into criminal networks and working with international partners, including the Australian Federal Police (“AFP”), to monitor the communications," the unsealed court record reads, referring to Anom, the app at the center of the investigation. Seamus Hughes, a researcher at George Washington University, shared the document with Motherboard.

> ***Do you know anything else about Anom? Were you a user? 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 AFP began going public with the contours of Anom Tuesday morning local time, and announced it had begun making arrests with data pulled from the honeypot.

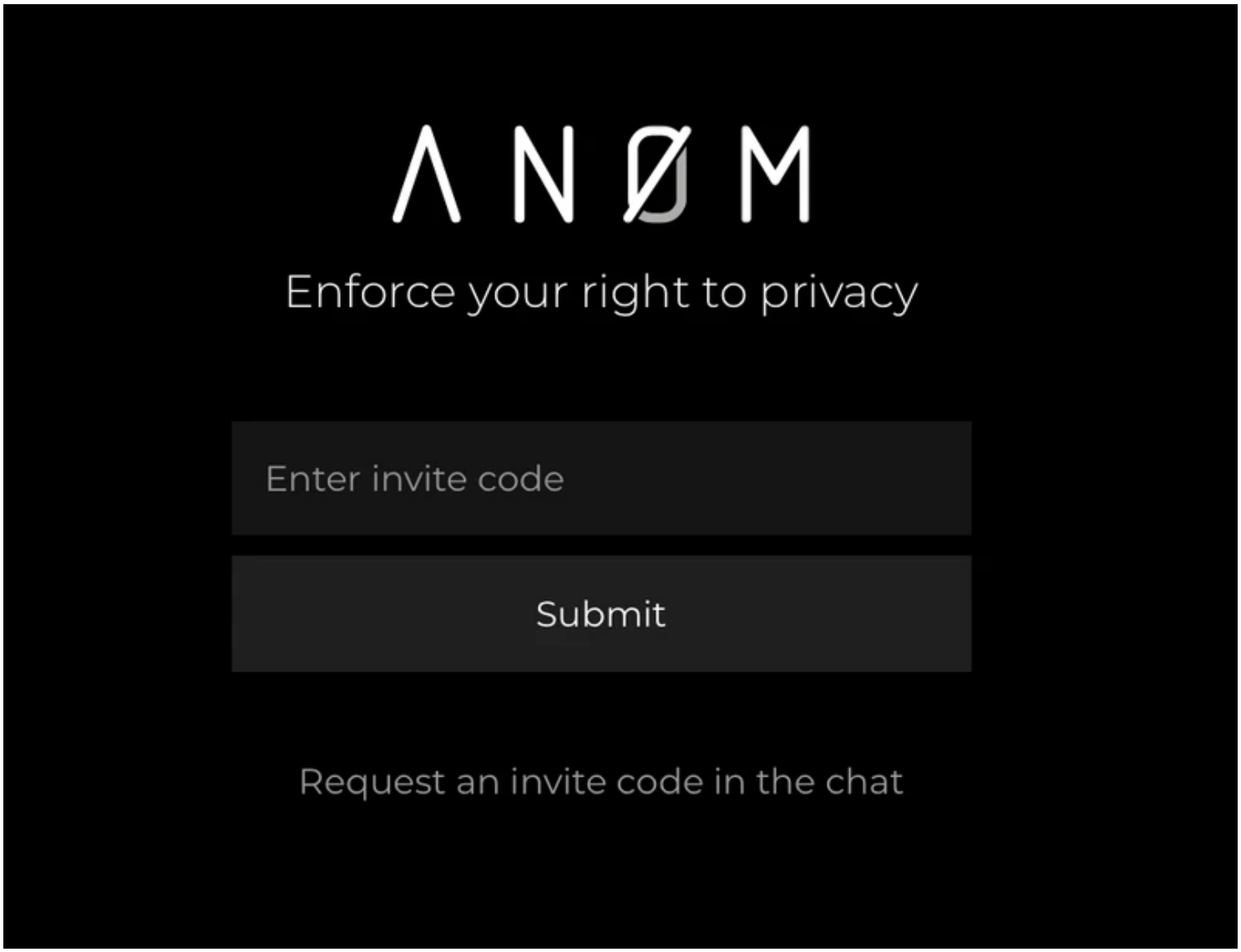
In 2018, the FBI arrested Vincent Ramos, the CEO of Phantom Secure, which provided custom, privacy-focused devices to organized criminals. In the wake of that arrest, a confidential human source (CHS) who previously sold phones on behalf of Phantom and another firm called Sky Global, was developing their own encrypted communications product. This CHS then "offered this next generation device, named 'Anom,' to the

FBI to use in ongoing and new investigations," the court document reads. While criminals left Phantom, they flocked to other offerings. One of those was Anom; the FBI started what it called Operation Trojan Shield, in which it effectively operated a communications network targeted to criminals and intercepted messages running across it.

The FBI, AFP, and CHS built the Anom system in such a way that a master key silently attached itself to every message set through the app, enabling "law enforcement to decrypt and store the message as it is transmitted," the document reads.

"A user of Anom is unaware of this capability," it adds.

But first the FBI and their source needed to establish Anom as an option in the criminal underworld. As Motherboard showed in a years-long investigation, using sources around Phantom as well as FBI files, Phantom was particularly popular in Australia. The CHS introduced Anom to his already trusted distributors of mobile devices, who were in turn trusted by criminal organizations, the document reads. Three people in Australia who had previously distributed Phantom, "seeing a huge payday," agreed to then sell these Anom devices, the document adds. With this, "the FBI aimed to grow the use of Anom organically through these networks," it reads.



A screenshot of the Anom site Motherboard took before Anom closed. Image: Motherboard.

Earlier on Monday before obtaining the court record, Motherboard reviewed Anom's social media presence. The company's Reddit account first announced the existence of the company two years ago, according to a since deleted but cached Reddit post that Motherboard found.

"Introducing Anom—a Ultra-Secure Mobile-Cell-Phone Messaging App for Android," the announcement read. "Your Confidentiality, Assured. Software hardened against targeted surveillance and intrusion—Anom Secure. Keep Secrets Safe!"

Anom started to grow, with initially 50 devices distributed in Australia and the AFP able to monitor the phones. It was slow at first, but soon word of the new devices spread, with Anom gathering several hundred users a year later, the document continued.

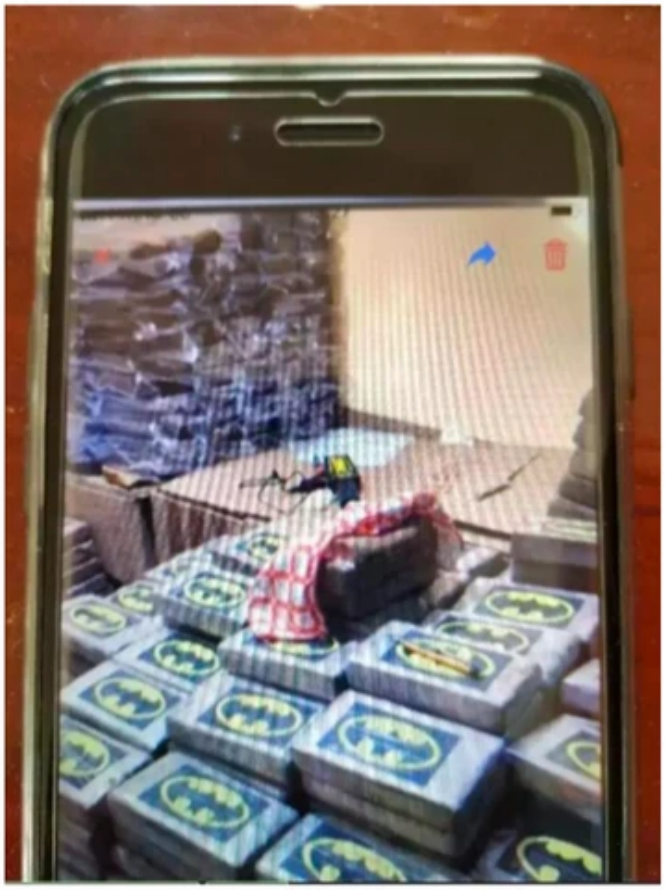
A third country also got involved in the investigation, and provided the FBI with Anom user data three times a week.

"This data comprises the encrypted messages of all of the users of Anoms with a few exceptions (e.g., the messages of approximately 15 Anom users in the U.S. sent to any other Anom device are not reviewed by the FBI)," the document reads.

Anom had grown exponentially in size, stretching beyond its Australian beginnings to having over 10,000 devices in over 90 countries. Germany, the Netherlands, Spain, and Serbia were also popular, with over 300 distinct transnational criminal organizations (TCOs) using the devices, the document reads. When authorities closed down Sky, as Motherboard reported in March, Anom's user base tripled.

The number of obtained messages totalled at over 20 million messages since October 2019. Messages include discussions around drug smuggling, corruption, and other high-level organized criminal activities. The document also includes direct quotes of messages from Anom users discussing cocaine shipments.

dreaming. You reckon. What he offer it to you for." Catanzariti then asked what Lupoi meant and whether Atlas sent the same photo in which atlas said it was all his. Lupoi said he never got the photo. Catanzariti responded that Lupoi was the one who sent it to him one month ago. Catanzariti then sent the following photo to Lupoi of Atlas's supply, which showed hundreds of kilograms of cocaine with a batman label.



A series of messages included in the court document. Image: Motherboard.

"There is 2kg put inside french diplomatic sealed envelopes out of Bogotta [sic]," one message reads referring to how the people are allegedly hiding shipments of cocaine.

"The Trojan Shield investigation has uncovered that Anom devices are used by TCOs to traffic drugs and launder the proceeds of those drug sales," the document reads. "The distributors of these devices also obstruct justice by remotely wiping the content of devices when law enforcement seizes them. Additionally, the review of Anom messages has initiated numerous high-level public corruption cases in several countries. The most prominent distributors are currently being investigated by the FBI for participating in an enterprise which promotes international drug trafficking, money laundering, and obstruction of justice."

The top five countries where Anom devices are currently used are Germany, the Netherlands, Spain, Australia, and Serbia.

A screenshot of a map showing what the FBI says its Anom's spread around the world. Image: Motherboard

Late Monday, the FBI said that it would be holding "a news conference announcing a massive worldwide takedown based on the San Diego FBI's unprecedented investigation involving the interception of encrypted communications" on Tuesday.

The Phantom, Sky, and Encrochat operations showed that law enforcement may shutdown or even hack into encrypted phone companies. But the Anom case shows that law enforcement will also go one step further: they will run such a network themselves. A previous DEA operation involved something similar but on a much smaller scale with BlackBerry devices.

"A goal of the Trojan Shield investigation is to shake the confidence in this entire industry because the FBI is willing and able to enter this space and monitor messages," the document reads.