European Police Malware Could Harvest GPS, Messages, Passwords, More

Joseph Cox ⋮ 5-6 minutes

The malware that French law enforcement deployed en masse onto Encrochat devices, a large encrypted phone network using Android phones, had the capability to harvest "all data stored within the device," and was expected to include chat messages, geolocation data, usernames, passwords, and more, according to a document obtained by Motherboard.

The document adds more specifics around the law enforcement hack and subsequent takedown of Encrochat earlier this year. Organized crime groups across Europe and the rest of the world heavily used the network before its seizure, in many cases to facilitate large scale drug trafficking. The operation is one of, if not the, largest law enforcement mass hacking operation to date, with investigators obtaining more than a hundred million encrypted messages.

"The NCA has been collaborating with the Gendarmerie on Encrochat for over 18 months, as the servers are hosted in France. The ultimate objective of this collaboration has been to identify and exploit any vulnerability in the service to obtain content," the document reads, referring to both the UK's National Crime Agency and one of the national police forces of France.

> ***Do you know anything else about Encrochat or impacted cases? 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***.***

As well as the geolocation, chat messages, and passwords, the law enforcement malware also told infected Encrochat devices to provide a list of WiFi access points near the device, the document reads.

"This command from the implant will result in the JIT receiving the MAC address which is the unique number allocated to each Wi-Fi access point and the SSID which is the human readable name given to that access point," the document adds. A JIT is a joint investigation team, made up of various law enforcement bodies.

Encrochat was a company that offered custom-built phones that sent end-to-end encrypted messages to one another. Encrochat took a base Android device, installed its own software, and physically removed the GPS, microphone, and camera functionality to lock down the devices further. These modifications may have impacted what sort of data the malware was actually able to obtain once deployed. Encrochat phones had a panic wipe feature, where if a user entered a particular PIN it would erase data stored on the device. The devices also ran two operating systems that sat side by side; one that appeared to be innocuous, and another that contained the users' more sensitive communications.

In a previous email to Motherboard a representative of Encrochat said the firm is a legitimate company with clients in 140 countries, and that it sets out "to find the best technology on the market to provide a reliable and secure service for any organization or individual that want[s] to secure their information." The firm had tens of thousands of users worldwide, and decided to shut itself down after discovering the hack against its network.

Encrochat's customers included a British hitman who assassinated a crime leader and an armed robber, and various violent gangs around Europe including those who used so-called "torture chambers." Some of the users may have been legitimate, however.

Since the shutdown, police across Europe have arrested hundreds of alleged criminals who used the service. Motherboard previously obtained chat logs that prosecutors have presented as evidence against one drug dealer.

Running an encrypted phone company is not typically illegal in-and-of-itself. The U.S. Department of Justice charged Vince Ramos, the CEO of another firm called Phantom Secure with racketeering conspiracy and other charges after an undercover investigation caught him saying the phones were made for drug trafficking. Phantom Secure started as a legitimate firm before catering more to the criminal market. Ramos was sentenced to nine years in prison in May 2019.

French authorities said at the time of the Encrochat shutdown that they had legal authority to deploy the mass hack, which they described as a "technical tool."

Previous Chapter Next Chapter