Encrypted Phone Firm Encrochat Used Signal Protocol

4-5 minutes

Image: Wanit Nantasuk / EyeEm

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

Encrypted phone firm Encrochat, whose customer base was primarily serious organized criminals, used the Signal protocol as part of its encrypted messaging application, according to a law enforcement document obtained by Motherboard.

The news highlights what law enforcement agencies may increasingly do when confronted with robust, end-to-end encryption like that of Signal: unable to read the content of intercepted messages, authorities may turn to hacking the end-point device, or phone, itself to siphon communications. In the Encrochat case, French police deployed malware to Encrochat phones and obtained the content of users' messages.

"EncroChat encrypt their messages with the Signal Protocol. This is a commonly used encryption protocol that is freely available. I am unaware of any capability to decrypt messages encrypted using the Signal protocol," the document, written by a technical employee from the UK's National Crime Agency (NCA), reads.

> ***Did you work for Encrochat? Do you have any more documents related to Encrochat arrests? 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.***

Many people know Signal as a free encrypted messaging app. But the eponymous organization behind the app also makes the underlying cryptographic protocol's libraries available for anyone to use. Companies, like WhatsApp, also use the protocol in their products. The hacking operation against Encrochat does not present any security issues for the Signal app or protocol itself.

Encrochat took stock Android devices and loaded them with the company's own applications. The phones had a feature that would wipe the device's contents if the user entered a specific PIN, and also ran two operating systems side-by-side.

One appeared innocuous and resembled a normal version of Android. The other contained the Encrochat messaging application. Like other companies in the encrypted phone space, Encrochat's devices could cost thousands of dollars for an annual subscription.

A section of the law enforcement document mentioning the Signal protocol. Image: Motherboard.

For years British hitmen have used the devices, as well as drug gangs across the UK.

Last year, authorities managed to push a malicious update from Encrochat's server down to individual Encrochat devices, according to other law enforcement documents obtained by Motherboard. The malware could harvest the phone's GPS location, stored messages, passwords, and more information, Motherboard previously reported. In the wake of that large scale hacking operation, French police shared the collected data with multiple international law enforcement agencies, including the NCA as well as Dutch authorities. Police then carried out wide ranging raids and arrests, uncovering large scale drug trafficking operations, serious threats to life, and even a so-called torture chamber inside a sound-proofed shipping container with a dentist's chair.

A person in control of an Encrochat email address previously told Motherboard they shut down the network after discovering the hacking operation against their company.

Signal declined to comment about Encrochat's use of the Signal protocol. The NCA declined to comment. Encrochat did not respond to a request for comment.

Update: This piece has been updated to include a response from the NCA.

Subscribe to our cybersecurity podcast CYBER, here.