

# Two vendors now sell iPhone cracking technology – and police are buying

By Niall Kitson

Published: 2018-04-16 · Archived: 2026-04-06 00:18:26 UTC

Image: IDGNS

16 April 2018

Law enforcement interest in iPhone encryption-cracking hardware from two new companies is a strong indication that Apple no longer claims the mobile security high ground. “What this means, if it’s true, is that people who thought all of their communications were totally secure shouldn’t feel so confident going forward,” said Jack Gold, principal analyst with [J. Gold Associates](#). “But, then security has always been a tug of war between the ones implementing it and the ones trying to break it.” In February, [reports surfaced](#) that an Israel-based technology vendor, Cellebrite, had discovered a way to unlock encrypted iPhones running iOS 11 and were marketing the product to law enforcement and private forensics firms around the world. According to [a police warrant obtained by Forbes](#), the US Department of Homeland Security had been testing the technology.

Shortly thereafter, [Grayshift](#) emerged as a different company that had [developed an inexpensive black box that could unlock any iPhone](#). Last week [Motherboard reported](#) that local and regional US police departments and the federal government have been purchasing the technology.

Grayshift reportedly hired a former Apple security engineer.

Motherboard confirmed the use of Grayshift’s GrayKey de-encrypting device – a 4×4” box with two iPhone-compatible lightning cables – by reviewing police department interest via public records requests and emails obtained from federal agencies that revealed purchases of the device. The GrayKey box can apparently unlock an iPhone in about two hours if the owner used a four-digit passcode and three days or longer if a six-digit passcode was used.

Nate Cardozo, a senior staff attorney with the [Electronic Frontier Foundation](#) (EFF), a non-profit digital rights group, said he believes the reports that the iPhone’s encryption has been cracked. Otherwise, if it were not true, law enforcement agencies wouldn’t be purchasing the hacking technology.

“The FBI huffed and puffed and said couldn’t get into the iPhone, and then we found out that’s not true... the literal night before the court hearing [to decide the case],” Cardozo said.

He was referring to the investigation of San Bernardino gunman Syed Rizwan Farook. Until last month, FBI Director Christopher Wray had maintained his agency [was unable to crack](#) the passcode on an iPhone used by Farook.

The Justice Department [had petitioned the courts](#) to force Apple to comply with an order to unlock the device; a judge granted the request, but delayed making a final decision until hearing arguments from both sides. The evening before a court hearing to decide the matter, the agency announced it had gotten help from an outside group. That [now appears not to be true](#).

The FBI's attempts to get Apple to help with unencrypting the iPhone were rebuffed. Apple maintained that [to break into one iPhone](#) would weaken security for all others.

The news that two iPhone unencrypting methods are now widely available to government agencies did not surprise analysts, who said it was inevitable.

“There is no such thing as unbreakable encryption,” Gold said. “The idea is to make it as hard as possible by adding layers of encryption or long keys to encode, decode. But a determined decoder can crack it, given enough tools and enough time.”

The GrayKey box retails for \$15,000. That model is geofenced to a specific location, requiring an internet connection that enables up to 300 unlocks. There is also a \$30,000 GrayKey model that can be used independent of internet connectivity and offers an unlimited number of device unlocks, according to *Motherboard*.

Conversely, Cellebrite charges \$5,000 to unlock a single iPhone, according to [Malwarebytes](#).

EFF's Cardozo said consumers shouldn't be overly concerned that iPhone breaking technology has become real because law enforcement agencies must still obtain a court-issued warrant to unlock a device.

But those concerned about privacy rights should realize that once cracking technology is available, it's reasonable to believe law enforcement agencies won't be the only ones to gain access to it.

“If you believe the only people will access to GreyKey or Celebrate are the cops, I've got a bridge to sell you,” Cardozo said.

*IDG News Service*

**Read More:** [Apple infosec iPhone security](#)