Shadowy hacking industry may be helping FBI crack an iPhone

24 March 2016, by Bree Fowler And Brandon Bailey

In a Wednesday, Dec. 7, 2011, file photo, a person stands near the Apple logo at the company's store in Grand Central Terminal, in New York. There's a shadowy global industry devoted to unlocking phones and extracting their information. For digital forensics companies, success can mean big bucks in the form of government contracts. And the notoriety that could come with cracking an iPhone used by a purported terrorist could rocket them to cyber stardom. (AP Photo/Mark Lennihan, File)

Turns out there's a shadowy global industry devoted to breaking into smartphones and extracting their information. But you've probably never heard of it unless you're a worried parent, a betrayed spouse—or a federal law enforcement agency.

Now one of those hacking businesses may well be helping the FBI try to break into the iPhone of one of the San Bernardino killers.

Late Monday, the FBI abruptly put its legal fight with Apple on hold, announcing that an "outside party" had come forward with a possible way to unlock the phone. In an update for reporters Thursday, FBI Director James Comey said the method "may work." If so, it could render Apple's forced cooperation unnecessary.

The announcement has thrown a spotlight on a group of digital forensics companies, contractors and freelance consultants that make a living cracking security protections on phones and computers. Comey said the publicity around the Apple case encouraged such people to come forward with new ideas.

Most such companies keep a very low profile. Since the bulk of their business is with governments and law enforcement, there's no reason to for them to advertise their services. In addition, it's in their interest to keep exactly what they do under wraps, said Christopher Soghoian, principal technology expert for the ACLU.

"The companies won't share their secrets. It's their special sauce," Soghoian said. "And they certainly won't tell Apple how they're doing what they're doing."

For the moment, no one outside the Justice Department appears to know who the FBI's white knight is. A great deal of speculation centers on Cellebrite—an Israel-based forensics firm that says it does business with thousands of law enforcement and intelligence agencies, militaries and governments in more than 90 countries—though it remains one of several possible candidates. A company spokesman declined to comment.

Cellebrite, founded in 1999, has contracts with the FBI dating back to at least 2013. The firm makes devices that allow law enforcement to extract and decode data such as contacts, pictures and text messages from more than 15,000 kinds of smartphones and other mobile devices.

It also makes commercial products that companies can use to help their customers transfer data from old phones to new ones. Apple even uses Cellebrite devices in some of its stores.

In the cybersecurity arms race, Apple has managed to stay ahead of these forensics companies. Cellebrite's website says its commercial tools work with iPhones running older operating systems, including iOS 8, but not the latest version, iOS 9, which is on the San Bernardino phone.

Of course, it's possible that one of these companies has made a breakthrough.

"Anything is crackable—it's just how much time do you have and how much money do you have to spend," said Jeremy Kirby, sales director at Susteen, a Cellebrite competitor in Irvine, California, that says it's not the FBI's outside party.

Susteen started as a software developer that made tools for cellphone companies. Kirby said his firm began developing forensic products for law enforcement about 10 years ago, after the FBI asked it to produce a tool that could preserve cellphone data for criminal investigations.

Now the company says its products are used by the Defense Department and hundreds of law enforcement agencies nationwide. It also sells a less-powerful data-extraction tool for consumers who want to check up on their kids or spouses by seeing their text messages, emails, smartphone photos and even deleted files.

Forensics companies maintain their own research staffs that probe target devices for weak spots, but for tough jobs, they sometimes turn to freelance hackers, some of whom will work for the highest bidder.

"What we're seeing now is what you can't do for yourself, you can buy," said Zuk Avraham, founder of the mobile security firm Zimperium, which seeks to defend phones against hacking.

Inspired by the FBI-Apple standoff, Rook Security, an Indianapolis-based cybersecurity firm that works with law enforcement, formed an expert team devoted to creating a copy of an iPhone's flash memory , hoping a backup would allow investigators to restore data that could be wiped out after too many wrong password guesses.

Many security researchers think that might work, though no one has announced success or demonstrated it on an iPhone running iOS 9 or higher. Rook, however, suspended its efforts when it couldn't find a way to take the phone apart without damaging it.

Avraham said he has no doubt the San Bernardino iPhone can be hacked.

"It's only a matter of time and resources," he said. "We have seen so many times when security researchers claim something to be impossible. They're proven wrong over time."

© 2016 The Associated Press. All rights reserved.

APA citation: Shadowy hacking industry may be helping FBI crack an iPhone (2016, March 24) retrieved 28 November 2022 from https://phys.org/news/2016-03-shadowy-hacking-industry-fbi-iphone.html

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.