NEWSFACTOR

FBI Won’t Reveal Vulnerability that Unlocked iPhone

Shirley Siluk

April 27, 2016

Although the White House has a policy to disclose some cyber vulnerabilities discovered by government agencies, the Federal Bureau of Investigation has indicated it will not reveal details about the security flaw that enabled it to unlock an iPhone connected to its investigation of a mass shooting in San Bernardino, Calif., in December.

According to "people familiar with the matter," the FBI will not provide Apple with details about the method it used, "leaving the company in the dark on a security vulnerability on some iPhone models," the Wall Street Journal reported yesterday. The paper also reported that the agency plans to inform the White House shortly that "it knows so little about the hacking tool . . . that it doesn't make sense to launch an internal government review" into whether Apple should be informed.

Many cybersecurity and privacy experts have since responded to that report with strong criticisms about the FBI's stance. "How does the FBI get to decide whether or not their iPhone [zero]-day should be submitted to the multi-agency review?" Christopher Soghoian, principal technologist and a senior policy analyst with the ACLU Speech, Privacy and Technology Project, asked on Twitter.

Apple did not respond to our requests for comment today. However, through an FBI spokesperson, FBI executive assistant director for science and technology Amy Hess told us today by e-mail that the Vulnerabilities Equities Process (VEP) is a disciplined, rigorous and high-level interagency decision-making process for vulnerability disclosure.

"The FBI assesses that it cannot submit the method to the VEP. The FBI purchased the method from an outside party so that we could unlock the San Bernardino device," Hess said through the spokesperson. "We did not, however, purchase the rights to technical details about how the method functions, or the nature and extent of any vulnerability upon which the method may rely in order to operate. As a result, currently we do not have enough technical information about any vulnerability that would permit any meaningful review under the VEP process."

At Least $1.3 Million for iPhone Hack

Earlier this month, reports emerged that the FBI paid "gray-hat" hackers for a zero-day vulnerability that enabled the agency to break into an iPhone 5c that had been used by Syed Rizwan Farook. Farook and his wife, Tashfeen Malik, carried out a December 2 shooting in San Bernardino that left 14 people dead. The pair was shot dead by police later that day.

During comments at a forum in London last week, FBI Director James Comey said his agency paid the hackers "more than I will make in the remainder of this job, which is seven years and four months, for sure." Based on what the director earns, that amount equates to more than $1.3 million.

Invoking the 1789 All Writs Act, the FBI had previously obtained a court order compelling Apple to write new code -- dubbed by many as "FBiOS" -- to help it bypass the device's built-in security. The agency abruptly withdrew that order late last month after revealing that an unnamed third party had allowed investigators to unlock the phone without Apple's help.

'Act of Recklessness'

The FBI's latest actions reported by the Wall Street Journal "should be taken as an act of recklessness," Jonathan Zdziarski, an iOS forensics security expert who has commented extensively on the FBI/Apple proceedings, wrote yesterday in a post on his blog.

While best practices in forensics science require that any tools used be tested and validated, Zdziarski noted, "The FBI apparently allowed an undocumented tool to run on a piece of high profile, terrorism-related evidence without having adequate knowledge of the specific function or the forensic soundness of the tool."

On Friday, the FBI also reversed course on a second iPhone investigation it had taken to court, withdrawing a request that Apple help it break into an iPhone connected with a drug-dealing case in New York. In its filing with the court, the Department of Justice (of which the FBI is a part) stated that "an individual" had provided a passcode that allowed the FBI to access that phone's contents and, "[a]ccordingly, the government no longer needs Apple's assistance to unlock the iPhone."

In his blog post, Zdziarski noted the New York case further suggests "the FBI's unwillingness or inability to do their job, to the degree of abusing the All Writs Act as an alternative to good police work."

"By its nature, the process by which the government considers whether to disclose or not disclose vulnerabilities must maintain confidentiality," the FBI's Hess said. "We therefore generally do not comment on whether a particular vulnerability was brought before the interagency and the results of any such deliberation. We recognize, however, the extraordinary nature of this particular case, the intense public interest in it, and the fact that the FBI already has disclosed publicly the existence of the method. Accordingly, we determined that it was appropriate to communicate with the interagency group, as well as the public about this important issue."

Hess added that the FBI has provided that information to the Equities Review Board that considers matters regarding the disclosure of vulnerabilities.

Paid for a 'Pig in a Poke'

Greg Nojeim, senior counsel and director of the Freedom, Security and Technology Project at the Center for Democracy & Technology, told us these latest developments led him to conclude, "They paid a million dollars for a pig in a poke."

Nojeim added that he was disappointed with the FBI's handling of the case, which indicated the agency failed the obtain the rights necessary to disclose the vulnerability. That raises questions about whether the third-party hackers remain free to sell their tool to other parties, he said.

"Certainly the FBI has the technical understanding, but they don't seem to be able to marshal it in an effective way," Nojeim said. "That tells the next seller they don't have to give up their rights and leaves the taxpayers on the hook." That establishes an even more troubling precedent, he added.

FBI Must Develop Own Exploits

“This whole debacle illustrates pretty starkly how badly the FBI has failed to build the in-house expertise it's going to need for 21st century investigations -- partly as a function of inadequate commitment of resources, partly because it's hard to recruit good hackers if occasional pot-smoking is a dealbreaker," Julian Sanchez, founding editor of the policy blog Just Security and a senior fellow at the libertarian Cato Institute, told us.

In the long run, it would cheaper than the ad hoc payouts for the San Bernardino exploit, and certainly more responsible than injecting massive capital into the global exploit market, he added.

“In this case, even after shelling out a reported $1.2 million, the FBI appears not to understand the technical details of the exploit they've purchased -- which could certainly be a problem in the future when the government actually obtains useful evidence it wants to be admissible in court,” Sanchez said. "It also means they're unable to help developers close those vulnerabilities in future updates -- which may make things easier for the FBI, but leaves the rest of the global user base vulnerable to any hacker or foreign government that's able to discover or purchase the same exploit."

Sanchez said it's long past time FBI officials gave up wishing for Congress to somehow magically "solve" the encryption "problem" for them and started developing the in-house capabilities needed to develop their own exploits. Then once the appropriate investigative use has been made of them -- helping developers develop defenses against them, he said.