FBI breaks iPhone security to uncover Pensacola shooter & Al Qaeda link [u]

By Malcolm Owen
5 months ago

The gunman at the center of the Pensacola shooting had links to Al Qaeda, the FBI investigation has uncovered, with the details claimed to have been sourced from iPhones that the government unlocked without Apple's assistance.

The FBI has determined Second Lt. Mohammed Saeed Alshamrani, a cadet from the Saudi Air Force training with the American military and the gunman of December's shooting in Pensacola, FL, was in communication with the terrorist group Al Qaeda. Two officials who were not authorized to speak about the evidence ahead of a planned press conference advised the information came from iPhones owned by Alshamrani.

While the evidence points to communication with the Al Qaeda operative, the *New York Times* reports it is unclear whether the shooter was given orders by their contact. Officials added the shooter was also in contact with the group repeatedly, including with members of its leadership, up until the attack took place.

The officials admitted the FBI managed to bypass security on one of Alshamrani's two iPhones, without assistance from Apple beyond providing the contents of the assailant's iCloud.

Though the unlock method wasn't revealed, the fact that the FBI has been able to gain access to evidence would usually be thought to slightly reduce the pressure applied by the US government and law enforcement agencies upon Apple to provide more assistance beyond what is already offered by the iPhone maker. To US Attorney General William Barr, the press conference was an opportunity to try and increase that pressure.

During the Department of Justice press conference, Barr and FBI Director Christopher Wray confirmed the contents of two iPhones were uncovered in the investigation, not one.

"Thanks to the great work of the FBI — and no thanks to Apple — we were able to unlock Alshamrani's phones," said Barr. "The trove of information found on these phones has proven to be invaluable to this ongoing investigation and critical security of the American people, however, if not for our FBI's ingenuity, some luck, and hours upon hours of time and resources, this information would have remained undiscovered."

Barr continued his attack on Apple and other tech companies wanting to maintain encryption policies as they are, declaring "The bottom line: our national security cannot remain in the hands of big corporations who put dollars over lawful access and public safety. The time has come for a legislative solution."

It is unknown when the FBI gained access, but it was within the last three months, as a report from early February indicated investigators had yet to bypass security applied to the iPhones. Despite demands of Apple from the FBI and US Attorney General William Barr failing to convince Apple to change its policies regarding device unlock assistance, the FBI evidently managed to find a way through a third-party method.

While Apple provided assistance to the investigation, including iCloud backups and "transactional data," it refused to offer assistance to break the encryption of its hardware and software to provide further access.

Given the use of exploits from security companies, evidently the FBI now has methods to gain access without needing to apply more pressure on Apple directly, and it will greatly affect the ever-ongoing encryption debate.

Strong-arming encryption

In a similar manner to the 2015 San Bernardino shooting stoked the fires of the encryption debate, the requests from law enforcement for Apple to hamper its own encryption to benefit governments rose following Pensacola.

In Barr's public request to Apple, he claimed the company provided no "substantive assistance" to the investigation. At the time of the January request, Burr also asserted "This situation perfectly illustrates why it is critical that the public be able to get access to digital evidence."

Barr's comments echoed previous calls from the US Attorney General for tech companies to provide access, nine months prior. At that time, Barr suggested encryption imposed "huge costs on society" and seriously "degrades the ability for law enforcement to detect and prevent crime before it occurs," along with hampering the ability for investigators to identify suspects and to successfully prosecute guilty parties.

It was insisted by Barr that the problem of encryption will exponentially increase as the use of "warrant-proof encryption" accelerates, and would "embolden" criminals who believe they cannot be caught.

"We are confident that there are technical solutions that will allow lawful access to encrypted data and communications by law enforcement," believed Barr, "without materially weakening the security provided by encryption."

In effect, Barr was demanding the creation of backdoors to weaken encryption, but just for law enforcement purposes. Critics of such claims insist the creation of a backdoor isn't worth exploring, as the same backdoor could be abused by criminals or for unintended purposes, such as mass surveillance operations.

Such requests are not limited only to the United States, with other security agencies like the UK's GCHQ examining ways to do the same thing.

Existing entrypoints

The continued debate may quieten down temporary, as it demonstrates there are opportunities for members of law enforcement to be able to gain access to data on encrypted devices, albeit without the assistance of the manufacturer.

Tools from companies such as GrayKey and Cellebrite take advantage of exploits and hacks to bypass the security of a device, as well as to facilitate the extraction of potential evidence. These hacks can be expensive, with some GrayKey tools costing as much as $30,000 at one point, making them only viable for governments and organizations with deep pockets.

Earlier in May, security firm and exploit-seller Zerodium claimed it had a surplus of exploits available for iOS, which it intended to sell to government agencies.

The availability of these tools do indicate that there are ways to beat Apple's security, albeit with a high degree of difficulty. The more recent claims also point to there being an ever-evolving array of methods available to law enforcement agencies willing to pay for the tools, despite Apple's best efforts to secure its products.

Update: Comments from William Barr added to the story following the press conference.