WhatsApp flaw let spies take control with calls alone (Update)

14 May 2019, by Frank Bajak And Raphael Satter

This Thursday, Aug. 25, 2016 file photo shows the logo of the Israeli NSO Group company on a building where they had offices in Herzliya, Israel. Spyware crafted by a sophisticated group of hackers-for-hire took advantage of a flaw in the popular WhatsApp communications program to remotely hijack dozens of phones, the company said late Monday. The Financial Times identified the actor as Israel's NSO Group, and WhatsApp all but confirmed the identification, describing hackers as "a private company that has been known to work with governments to deliver spyware.(AP Photo/Daniella Cheslow, File)

Spyware crafted by a sophisticated group of hackers-for-hire took advantage of a flaw in the popular WhatsApp communications program to remotely hijack dozens of targeted phones without any user interaction.

The Financial Times identified the hacking group as Israel's NSO Group, which has been widely condemned for selling surveillance tools to repressive governments.

WhatsApp all but confirmed the identification, describing hackers as "a private company that has been known to work with governments to deliver spyware." A spokesman for the Facebook subsidiary later said: "We're certainly not refuting any of the coverage you've seen."

The spyware did not directly affect the end-to-end encryption that makes WhatsApp chats and calls private. It merely used a bug in the WhatsApp software as an infection vehicle. The malware allows spies to effectively take control of a phone—remotely and surreptitiously controlling its cameras and microphones and vacuuming up personal and geolocation data. Encryption is worthless once a phone's operating system has been violated.

Hackers are always looking for flaws in apps and operating systems that they can exploit to deliver spyware. State-run intelligence agencies including the U.S. National Security Agency invest tens of millions on it. Indeed, Google's ProjectZero bug-hunting team scoured WhatsApp last year looking for vulnerabilities but did not find any. Instead, it was WhatsApp's security team that found the flaw.

The development comes as Facebook looks to triple down on its messaging services by merging WhatsApp, Facebook Messenger and Instagram Direct and bringing WhatsApp-level encryption to the others. The attack would not affect Facebook's ability to do that.

The malware was able to penetrate phones through missed calls alone using the app's voice calling function, said the WhatsApp spokesman, who was not authorized to be quoted by name. He said an unknown number of people—an amount in the dozens at least would not be inaccurate—were infected with the malware, which the company discovered in early May, the spokesman said.

John Scott-Railton, a researcher with the internet watchdog Citizen Lab, called the hack "a very scary vulnerability."

"There's nothing a user could have done here,

short of not having the app," he said. The vast majority of hacks involve some sort of user interaction, such as clicking on an infected link.

The WhatsApp spokesman said its flaw was discovered while "our team was putting some additional security enhancements to our voice calls." He said engineers found that people targeted for infection "might get one or two calls from a number that is not familiar to them. In the process of calling, this code gets shipped."

WhatsApp, which has more than 1.5 billion users, immediately contacted Citizen Lab and human rights groups, quickly fixed the issue and pushed out a patch. He said WhatsApp also provided information to U.S. law enforcement officials to assist in their investigations.

This Friday, March 10, 2017, file photo shows the WhatsApp communications app on a smartphone, in New York. WhatsApp says a vulnerability in the popular communications app let mobile phones be infected with sophisticated spyware with a missed in-app call alone. (AP Photo/Patrick Sison, File)

"We are deeply concerned about the abuse of such capabilities," WhatsApp said in a statement.

Although WhatsApp urged all users to update the program on their phones, only a minuscule percentage run the risk of being targeted by such malware.

NSO said in a statement that its technology is used by law enforcement and intelligence agencies to fight "crime and terror."

"We investigate any credible allegations of misuse and if necessary, we take action, including shutting down the system," the statement said. A spokesman for Stephen Peel, whose private equity firm Novalpina recently announced the purchase of part of NSO, did not return an email seeking comment.

The revelation adds to the questions over the reach of the Israeli company's powerful spyware.

Prior to the latest WhatsApp revelation, NSO's spyware has repeatedly been found deployed to hack journalists, lawyers, human rights defenders and dissidents. Most notably, the spyware was implicated in the gruesome killing of Saudi journalist Jamal Khashoggi, who was dismembered in the Saudi consulate in Istanbul last year and whose body has never been found.

Several alleged targets of the spyware, including a close friend of Khashoggi and several Mexican civil society figures, are currently suing NSO in an Israeli court over the hacking.

On Monday, Amnesty International—which said last year that one its staffers was also targeted with the spyware—said it would join in a legal bid to force Israel's Ministry of Defense to suspend NSO's export license.

That makes the discovery of the vulnerability particularly disturbing because one of the targets was a U.K.-based human rights lawyer, the attorney told The Associated Press.

The lawyer, who spoke on condition of anonymity for professional reasons, said he received several suspicious missed calls over the past few months, the most recent one on Sunday, only hours before WhatsApp issued the update to users fixing the flaw.

In its statement, NSO said it "would not or could not" use its own technology to target "any person or organization, including this individual."

More information: Frank Bajak: twitter.com/fbajak

Raphael Satter: twitter.com/razhael