PHYS.ORG

WhatsApp, security and spyware: what happened

May 17 2019

Credit: CC0 Public Domain

Facebook-owned WhatsApp's revelation of a security flaw allowing hackers to inject spyware on smartphones raised fresh concerns about the security of the mobile ecosystem.

Here are five key questions and answers:

What happened to WhatsApp?

The security hole in the WhatsApp messaging app could enable an attacker to inject malware to gain access to Android or Apple smartphones.

WhatsApp patched the flaw this week after being informed that the spyware was being used to track human rights activists and lawyers.

Security researchers believe the attackers used the powerful Pegasus spyware from Israel-based NSO Group. According to a recent analysis of the software by the security firm Lookout, Pegasus can "subvert" the device's security and "steals the victim's contact list and GPS location, as well as personal, Wi-Fi, and router passwords stored on the device."

The infection could take root with a simple call through WhatsApp. To make matters worse, victims may not know their phones were infected because the malware allowed attackers to erase call histories.

This delivery was "particularly scary," said security researcher John Dickson of the Denim Group, because it infected devices without any user action.

"Normally a user has to click on something or go to a site, but that wasn't the case here," Dickson said. "And once (the attacker) is in, they own the device, they can do anything."

Who is to blame?

While the flaw was discovered in WhatsApp, security experts say any application could have been a "vehicle" for the spyware payload.

"We have not yet been able to write software that doesn't have bugs or flaws," said Joseph Hall, chief technologist for the Center for Democracy & Technology, a digital rights group.

Hall said the encryption in WhatsApp was not broken and that "Facebook's response was exceedingly fast."

Marc Lueck of the security firm Zscaler said that based on Facebook's response, "You should give them kudos for discovering it in the first place, this was a very deep vulnerability."

The intrusion at WhatsApp "wasn't an attack on encryption, it was an attack on another element of the application" said Lueck.

Is encryption still worthwhile?

Encryption remains an important feature by establishing a secure "tunnel" between two parties that verifies their identities, Lueck noted.

"Encryption isn't important just for privacy, it's important for trust," he said.

Encryption used by WhatsApp and other messaging applications prevents eavesdropping on messages and conversations but does not protect against an attack that gains access to the device itself, researchers note.

"End to end encryption does nothing to protect against attacks on your endpoint, true. And seatbelts and airbags do nothing to prevent your car from being hit by a meteorite," tweeted Matt Blaze, a Georgetown University computer security expert.

"While neither protects against every possible harm, they both remain the most effective defenses against very common harm."

Dickson said that while no encryption is foolproof, the only way to completely avoid hacking would be to avoid electronics entirely: "You could use guys on horseback."

Should I worry about being attacked?

Citizen Lab, a research center at the University of Toronto, said in a 2018 report that it found Pegasus spyware infections in 45 countries, with 36 "probable government operators."

NSO maintains it delivers its software for legitimate law enforcement and intelligence purposes. But the Toronto researchers said it had been obtained by countries with "dubious" human rights records and suggested it may have been used by Saudi Arabia to track and kill dissident journalist Jamal Khashoggi.

Citizen Lab researchers wrote in the Globe & Mail that they "unearthed at least 25 cases of abusive targeting of advocacy groups, lawyers, scientists and researchers, investigators into mass disappearances and media members."

But Lueck said programs such as Pegasus are extremely costly and cannot easily be monetized by hackers for profit.

"Your average person is not the target of this specific piece of software, which is built to sell to governments to target individuals and doesn't work on a large scale," he said.

Still, Lueck said the flaw underscores the fact that "the mobile phone ecosystem has become as insecure and as vulnerable a platform as the computer."

Do governments need better digital tools?

The revelations come as governments seek better tools to track criminals and extremists using encrypted messaging. An Australian law requires tech giants to remove electronic protections and help with access to devices or services.

Law enforcement agencies have complained of "going dark" in the face of encrypted electronic communications as they investigate serious crimes like terrorism and child sex offenses.

But Hall said that the news about Pegasus shows governments have tools to exploit software flaws for specific targeting without weakening encryption and privacy for all users.

"You can target the delivery at specific people rather than breaking into everyone's phone at once," he said.

Citation: WhatsApp, security and spyware: what happened (2019, May 17) retrieved 23 June 2024 from https://phys.org/news/2019-05-whatsapp-spyware.html