WhatsApp sues Israeli firm NSO over cyberespionage

29 October 2019, by Glenn Chapman

WhatsApp said some users of the messaging app were targeted with spyware, and filed suit against an Israeli firm said to be behind the attack

WhatsApp on Tuesday sued Israeli technology firm NSO Group, accusing it of using the Facebook-owned messaging service to conduct cyberespionage on journalists, human rights activists and others.

The suit filed in a California federal court contended that NSO Group tried to infect approximately 1,400 "target devices" with malicious software to steal valuable information from those using the messaging app.

WhatsApp head Will Cathcart said the lawsuit was filed after an investigation showed the Israeli firm's role the cyberattack, despite its denials.

"NSO Group claims they responsibly serve governments, but we found more than 100 human rights defenders and journalists targeted in an attack last May. This abuse must be stopped," Cathcart said on Twitter.

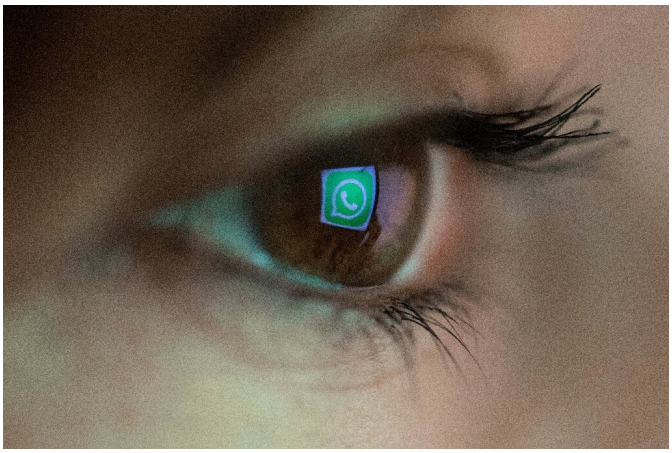
The lawsuit said the software developed by NSO known as Pegasus was designed to be remotely installed to hijack devices using the Android, iOS, and BlackBerry operating systems.

The complaint said the attackers "reverse-engineered the WhatsApp app and developed a program to enable them to emulate legitimate WhatsApp network traffic in order to transmit malicious code" to take over the devices.

"While their attack was highly sophisticated, their attempts to cover their tracks were not entirely successful," Cathcart said in an opinion piece published in the Washington Post, noting that the investigation found internet-hosting services and accounts associated with NSO.

The suit calls on court to order NSO Group to stop any such attacks and asks for unspecified damages.

WhatsApp in May called on users to upgrade the application to plug a security hole that allowed for the injection of sophisticated malware that could be used for spying at the messaging app used by 1.5 billion people around the world.



WhatsApp said its investigation traced a cyberespionage effort back to the Israeli technology firm NSO Group

said.

The malicious code was transmitted through WhatsApp servers from about April 29 to May 10, targeting devices of attorneys, journalists, human rights activists, political dissidents, diplomats, and other senior foreign government officials, according to the complaint.

"A user would receive what appeared to be a video call, but this was not a normal call," Cathcart said of the cyberattack.

"After the phone rang, the attacker secretly transmitted malicious code in an effort to infect the victim's phone with spyware. The person did not even have to answer the call."

Fighting 'crime and terror'

The NSO Group came to prominence in 2016 when researchers accused it of helping spy on an activist in the United Arab Emirates.

Its best-known product is Pegasus, a highly invasive tool that can reportedly switch on a target's phone camera and microphone, and access data on it.

The firm has been adamant that it only licenses its software to governments for "fighting crime and terror" and that it investigates credible allegations of misuse, but activists argue the technology has been instead used for human rights abuses.

Danna Ingleton of Amnesty International said the results of the WhatsApp investigation "underscore that NSO Group continues to profit from its spyware products being used to intimidate, track, and punish scores of human rights defenders across the globe, including the Kingdom of Bahrain, the United Arab Emirates and Mexico."

Ingleton said Amesty and other groups are seeking in the Israeli courts to block NSO for exporting the technology.

"WhatsApp deserves credit for their tough stance against these malicious attacks, including their efforts to hold NSO to account in the courts," she