WhatsApp says journalists and civil society members were targets of Israeli spyware

Stephanie Kirchgaessner ⋮ 6-7 minutes ⋮ 1/31/2025

Nearly 100 journalists and other members of civil society using WhatsApp, the popular messaging app owned by Meta, were targeted by spyware owned by Paragon Solutions, an Israeli maker of hacking software, the company alleged on Friday.

The journalists and other civil society members were being alerted of a possible breach of their devices, with WhatsApp telling the Guardian it had “high confidence” that the 90 users in question had been targeted and “possibly compromised”.

It is not clear who was behind the attack. Like other spyware makers, Paragon’s hacking software is used by government clients and WhatsApp said it had not been able to identify the clients who ordered the alleged attacks.

Experts said the targeting was a “zero-click” attack, which means targets would not have had to click on any malicious links to be infected.

WhatsApp declined to disclose where the journalists and members of civil society were based, including whether they were based in the US.

Paragon has a US office in Chantilly, Virginia. The company has faced recent scrutiny after Wired magazine in October reported that it had entered into a $2m contract with the US Immigration and Customs Enforcement’s homeland security investigations division.

The division reportedly issued a stop-work order for the contract to verify whether it complied with a Biden administration executive order that restricted the use of spyware by the federal government. The Trump administration has revoked dozens of the Biden administration’s executive orders in its first two weeks in office, but the 2023 order, which prohibited the use of spyware that posed a risk to national security remains in effect.

WhatsApp said it had sent Paragon a “cease and desist” letter and that it was exploring its legal options. WhatsApp said the alleged attacks had been disrupted in December and that it was not clear how long the targets may have been under threat.

The company is currently notifying victims of the alleged hacking, who will be contacted by WhatsApp.

“WhatsApp has disrupted a spyware campaign by Paragon that targeted a number of users including journalists and members of civil society. We’ve reached out directly to people who we believe were affected. This is the latest example of why spyware companies must be held accountable for their unlawful actions. WhatsApp will continue to protect people’s ability to communicate privately,” a company spokesperson said.

Paragon Solutions declined to comment.

A person close to the company told the Guardian that Paragon had 35 government customers, that all of them could be considered democratic, and that Paragon did not do business with countries, including some democracies, that have previously been accused of abusing spyware. The person said that included Greece, Poland, Hungary, Mexico and India.

Paragon’s spyware is known as Graphite and has capabilities that are comparable to NSO Group’s Pegasus spyware. Once a phone is infected with Graphite, the operator of the spyware has total access to the phone, including being able to read messages that are sent via encrypted applications like WhatsApp and Signal.

The company, which was founded by the former Israeli prime minister Ehud Barak, has been the subject of media reports in Israel recently, after it was reported that the group was sold to a US private equity firm, AE Industrial Partners, for $900m.

Reports suggested the deal had not yet received full regulatory approval in Israel. Cyberweapons like Graphite and Pegasus are regulated by the Israeli ministry of defence. The Guardian reached out to AE Industrial Partners, which is based in Boca Raton, Florida. Paragon is not listed among the company's investments on its website.

"For some time Paragon has had the reputation of a 'better' spyware company not implicated in obvious abuses, but WhatsApp's recent revelations suggest otherwise. This is not just a question of some bad apples – these types of abuses are a feature of the commercial spyware industry," said Natalia Krapiva, senior tech legal counsel at Access Now.

WhatsApp said it believed the so-called vector, or means by which the infection was delivered to users, was through a malicious pdf file that was sent to individuals who were added to group chats. WhatsApp said it could say with "confidence" that Paragon was linked to this targeting.

John Scott-Railton, a senior researcher at the Citizen Lab at the University of Toronto, which tracks and identifies digital threats against civil society, said Citizen Lab provided WhatsApp with some information that helped the company understand the vector that was used against the company's users.

The group is expected to publish a report in the future that will provide more details about the alleged targeting.

WhatsApp announced the news just weeks after a judge in California ruled in the company's favor in a landmark case against NSO Group, the high-profile spyware maker that in 2021 was placed by the Biden administration on a commerce department blacklist. At the time, the Biden administration said it had placed NSO on the so-called entity list because the company had engaged in activities "that are contrary to the national security or foreign policy interests of the United States".

NSO has lobbied members of Congress to be taken off the list.

WhatsApp filed a lawsuit against NSO in 2019 after it said 1,400 users had been infected by the company's spyware. In December, a judge, Phyllis Hamilton, ruled that NSO was liable for the attacks, and that NSO had violated state and federal US hacking laws and WhatsApp's own terms of service.

Have you been affected? If so please contact
Stephanie.Kirchgaessner@theguardian.com