United Nations official and others in Armenia hacked by NSO Group spyware

Publication Date: 2023-05-25

Author: Stephanie Kirchgaessner

Section: Technology

Tags: Hacking, Armenia, Europe, news

Article URL: https://www.theguardian.com/technology/2023/may/25/nso-group-spyware-armenia-war

CYBER INTELLIGENCE FOR GLOBAL SECURITY AND STABILITY
NSO creates technology that helps government agencies prevent and investigate terrorism and crime to save thousands of lives around the globe.

Researchers have documented the first known case of NSO Group’s spyware being used in a military conflict after they discovered that journalists, human rights advocates, a United Nations official, and members of civil society in Armenia were hacked by a government using the spyware. The hacking campaign, which targeted at least a dozen victims from October 2020 to December 2022, appears closely linked to events in the long-running military conflict between Armenia and Azerbaijan over the contested Nagorno-Karabakh region. Previous investigations into spyware abuses by NSO Group’s clients have already established – with “substantial evidence”, according to researchers – that Azerbaijan is a government client of NSO Group. The news is significant because the use of Pegasus, a military-grade spyware that can hack into and remotely control any phone, has never been documented inside a military conflict. An NSO spokesperson said the company could not comment on the new report by Access Now and others because it had not been shared with NSO. It said that previous investigations into allegations of “improper use of our technologies” by clients resulted in the termination of multiple contracts. The investigation was conducted by researchers at Access Now, CyberHUB-AM, the Citizen Lab at the Munk School of Global Affairs at the University of Toronto, Amnesty International’s Security Lab, and Ruben Muradyan, an independent mobile security researcher. The hacking of the Armenia-based individuals was first discovered in November 2021, two months after a series of clashes along the Armenia-Azerbaijan border claimed at least 200 lives in the most serious escalation of violence since the 2020 Nagorno-Karabakh war. Apple began sending notifications to mobile phone users who they believed had been targeted with state-sponsored spyware. Anna Naghdalyan, a former Armenia foreign ministry spokesperson was hacked at least 27 times between October 2020 and July 2021, at a time when she was still serving as a spokesperson for the ministry. Researchers said the timing of the attacks put her “squarely in the most sensitive conversations and negotiations related to the Nagorno-Karabakh crisis”, including the ceasefire mediation attempts by France, Russia and the US and official visits to Moscow and Karabakh. Naghdalyan told Access Now that she had “all the information about the developments during the war on [her] phone” at the time of her hacking, and that she now feels there is no way for her to feel fully safe. “Even if you have the most secure system on your phone, you cannot be secure,” she said. Experts said the development showed the risks of spyware being used to add fuel to geopolitical fires. “This raises important questions about the safety of international organisations, journalists, humanitarians and others working around conflict. It should also send a chill down the spine of every foreign government whose diplomatic service has been engaged around the conflict,” said John Scott-Railton, a senior researcher at the Citizen Lab. Other victims include Karlen Aslanyan, a Radio Azatutyun journalist who was covering the Armenian political crisis that erupted after Armenia’s defeat in the 2020 conflict. At least one guest on

Aslanyan’s popular Armenian show – Kristinne Grigoryan – was hacked a month after she appeared on the programme. Another journalist, Astghik Bedevyan, who was closely covering the conflict, was also hacked in May 2021. The report lists several other journalists, professors and human rights defenders whose work centred on the military conflict. Access Now said that five of the 12 hacked individuals have elected to remain anonymous, but that they include a UN representative who does not have the UN’s consent to come forward. Access Now and its partners said they believe the hacking was done by a customer of NSO Group, though the data could not conclusively be linked to a specific client. They added that, given the individuals’ work on the conflict, it is possible that Armenia’s government may also have been interested in hacking the individuals, but said there was no other evidence to suggest that Armenia had ever been a Pegasus user. Indeed, the country is believed to be a user of a different spyware product named Predator, created by Cytrox, a business rival of NSO. Other evidence points to Azerbaijan as an NSO customer, including findings by the Citizen Lab that some Pegasus one-click infections linked to infrastructure that masqueraded as Azerbaijani political websites. Amnesty Tech’s research has also identified Azerbaijan-linked domains that point to Azerbaijan as a likely Pegasus customer. The embassies of Armenia and Azerbaijan in the US did not immediately respond to a request for comment. NSO has said it investigates credible reports of its spyware being abused by government clients. NSO Group was placed on a blacklist by the Biden administration in 2021, after the commerce department said it found the company had supplied its technology to foreign governments that used it to maliciously target government officials, journalists, business people, activists and embassy workers.