More political fallout from the Pegasus spyware revelations

Kevin Reed
3 August 2021

Political fallout from the exposure of government use of the Israeli-based NSO Pegasus spyware continued last week as protesters rallied to demand the resignation of the right-wing government in Hungary.

On July 26, approximately 1,000 people organized by opposition political parties demonstrated at the House of Terror museum in Budapest in response to revelations that the Hungarian government had been using the spyware to monitor the activity of journalists, businesspeople and politicians. The House of Terror museum is housed in the building where individuals were interrogated, tortured and murdered and contains exhibits about the victims of both the fascist and Stalinist regimes in the twentieth century.

The protesters demanded the resignation of Prime Minister Viktor Orbán and Justice Minister Judit Varga, who has the authority under Hungarian law to sign off on secret surveillance without judicial oversight.

The events in Budapest were touched off by investigative reporting two weeks ago from a consortium of 16 media outlets called the Pegasus Project that analyzed leaked documents showing that more than 50,000 individuals had been targeted by the software and potentially had their smartphones hacked and transformed into 24-hour per day surveillance devices. Among the countries these individuals come from are Hungary, Pakistan, Saudi Arabia, Mexico, Azerbaijan, India and France.

The software firm NSO Group developed Pegasus ostensibly as a tool for stopping "terrorists and criminals," but instead the leaked information showed that the numerous government customers of the Israeli firm were using the malware to spy on major political figures including sitting presidents and prime ministers and monarchs.

Headed up by the Paris-based Forbidden Stories and Amnesty International, the Pegasus Project—which also includes the *Washington Post* and the *Guardian*—performed forensic analysis on the smartphones of some of the individuals on the Pegasus target list and showed that their devices exhibited evidence of either hacking attempts or successful spyware installation.

While the leaked information included the phone numbers of approximately 300 Hungarian citizens, the forensic analysis demonstrated that Pegasus had been used to break into the smartphones of at least five Hungarian journalists. According to *InsightHungary*, for example, the smartphones of "Szabolcs Panyi and András Szabó of investigative reporting outfit Direkt36," had been broken into. The phones of opposition politician György Gémesi, who leads the New Start Party, and János Banáti, president of the Hungarian Bar Association, were also on the leaked list of Pegasus targets, but these devices did not undergo the forensic examination to confirm that they had been breached.

While the journalistic investigation points to the involvement of the Hungarian government in a spyware operation, *InsightHungary* reported on July 22 that government officials have neither confirmed nor denied the use of Pegasus. They did, however, state that "covert surveillance in Hungary occurs only in accordance with relevant laws."

Speaking in Brussels more directly on the subject without confirming the use of Pegasus, Justice Minister Varga said, "Let's not be ridiculous, every country needs such tools! It's an illusion if anyone tries to make an issue out of it." Additionally, Prime Minister Orbán's chief of staff told the press that the cabinet did not discuss the issue and had "no plans to conduct an investigation into the spying allegations," according to *InsightHungary*.

The political crisis in Hungary follows close behind that of the far-right regime of Narendra Modi in India, where approximately 1,000 people were targeted by the Pegasus tool, including journalists, activists, lawyers and

academics. Among the mobile numbers found on the leaked data list were two devices used by Congress leader Rahul Ghandi along with five of his close personal friends.

While NSO Group continues to absolve itself of any responsibility for the deployment of its hacking software by governments around the world—the company has refused to disclose a list of its 60 accounts within 40 or more state clients—the company has moved to block several governments from using Pegasus, pending an investigation of the allegations.

An anonymous NSO Group representative told NPR on July 29, "There is an investigation into some clients. Some of those clients have been temporarily suspended." The source added that NSO, "will no longer be responding to media inquiries on this matter and it will not play along with the vicious and slanderous campaign." The *Washington Post* reported that the clients that have been suspended include Saudi Arabia, Dubai in the United Arab Emirates and some public agencies in Mexico.

Cyber-security experts have identified Pegasus as one of the most powerful spyware tools developed and deployed to date. As opposed to previous techniques, which require a user to click on something contained in a text message or email in order to install the malware on the device, Pegasus is a "zero-click" hack that penetrates the security of a smartphone simply by sending a text message to it that does not even need to be opened by the user to infect their system.

Dr. Tim Stevens, director of the Cybersecurity Research Group at King's College London, explained the nature of zero-day vulnerabilities to BBC *Science Focus* magazine, "It is a fact that all very large pieces of software, like an operating system like Apple's iOS or Android or any other, including open source operating systems, have bugs. None of them are perfect. They present openings or opportunities for people to use to gain access.

"It's like locking up all the doors and windows, but leaving the kitchen window open overnight. If the burglar is going to recce the whole house, they will find it eventually, no matter how large your house. And that's exactly what goes on with software. ...

"Pegasus effectively jailbreaks your phone, it unlocks all this kind of administrative functionality that it then uses to position itself and hide itself and have access to everything that's going on in your phone. It's a very novel and impressive technical feat."

Once the spyware is on a smartphone, it can be used to monitor all activity within both the apps such as email, browser activity, text messaging and photo images as well as the hardware such as the microphone, speakers and front-facing and rear-facing cameras.

In response to the Pegasus leak revelations—which he called "the story of the year"—whistleblower and former intelligence analyst Edward Snowden published a blog post on Substack on July 26 titled, "The Insecurity Industry." In it, Snowden wrote that prior to the Pegasus revelations, "most smartphone manufacturers along with much of the world press collectively rolled their eyes at me whenever I publicly identified a fresh-out-of-the-box iPhone as a potentially lethal threat."

He went on to say that despite years of reporting that implicated NSO Group's "for-profit hacking of phones in the deaths and detentions of journalists and human rights defenders" and despite evidence that smartphone operating systems are "riddled with catastrophic security flaws," that he has often felt like "someone trying to convince their one friend who refuses to grow up to quit smoking and cut back on the booze—meanwhile, the magazine ads still say 'Nine of Ten Doctors Smoke iPhones!' and 'Unsecured Mobile Browsing is Refreshing!'"

Snowden, who has been living in asylum in Russia for more than eight years, exposed in 2013 the existence of a massive surveillance operation being run by the US National Security Agency and Central Intelligence Agency that was monitoring the electronic and phone activity of everyone on earth.

Of the Pegasus spyware, Snowden wrote in his blog post that he considered the leak and revelations about it to be a "turning point" and added that NSO Group and the global commercial hacking industry "involves cooking up new kinds of infections that will bypass the very latest digital vaccines—AKA security updates—and then selling them to countries that occupy the red-hot intersection of a Venn Diagram between 'desperately craves the tools of oppression' and 'sorely lacks the sophistication to produce them domestically.'" Snowden has called for this industry to be dismantled.