The NATIONAL INTEREST FOUNDATION

A New Report Finds that Israeli Firm NSO Group's Pegasus Spyware was Used to Target Democracy Advocates and Human Rights Defenders in Thailand

A new report released by internet watchdog organizations has shown that 30 Thai pro-democracy activists have been the target of Pegasus spyware. This is just the latest of the numerous accounts of the Israeli-made spyware being used to suppress pro-democracy and human rights activities. In this particular case, the group of individuals, including academics, activists, and civil society leaders, were being surveilled by an unknown entity according to a forensic investigation. The investigation was conducted by the Canadian group Citizen Lab and Thai non-governmental organizations (NGOs) iLaw and Digital Reach. It was triggered after the activists from Apple advised that they had been victims of state-sponsored attacks aimed at distributing malware. Pegasus spyware can be used to read text messages, as well as track calls and locations of the intended target. Citizen Lab could not definitively confirm that the Thai government was responsible, but circumstantial evidence points towards that being the case. There is at least one known operator of Pegasus in Thailand, and this fresh unveiling has strengthened calls for a global moratorium on the repressive spyware.

The Pegasus spyware was created by NSO Group, an Israeli technology firm, and is found to have been used to suppress pro-democracy advocates in countries across the world with repressive regimes. Similar occurrences have repeatedly been revealed multiple times despite NSO Group attempting to claim that they vet any government agency they sell the harmful spyware to. Though it is no surprise that repressive governments use spyware to monitor and try to quell pro-democracy advocates and activities, it is alarming to analysts and observers that the firm selling the spyware is tied and linked to the Israeli government itself.

The latest findings support the long-held notion that the Pegasus spyware is targeting human rights activists, political dissidents, journalists, and lawyers all over the globe. This surveillance violates their basic human rights, including the right to privacy, free speech, movement, and the ability to peacefully protest and organize. It has been over a decade since the Pegasus spyware was released, and there is still currently no moratorium against its sale to repressive regimes, despite calls for this to be put into place. NSO Group is therefore profiting from human rights violations around the world. Besides the new uncovering in Thailand, there have been other recently reported instances in Morocco, Poland, El Salvador, Israel, Palestine, and Spain. These are only the clearly known cases, and it is likely that there are many other instances of its use that have gone either unnoticed or unreported. Not only does this spyware violate fundamental human rights, it has also been implicated in the heinous murder of journalists such as Jamal Khashoggi. It was discovered that two people who were close to Khashoggi were targeted by the spyware before and after his assassination in October of 2018 at the hands of Saudi authorities.

Some steps have been taken to try and inhibit the use of Pegasus, including the Biden administration adding the NSO Group to a Commerce Department list of restricted companies. Unfortunately, NSO Group has been using its ill-gotten gains to launch a powerful lobbying campaign to get off of this list in order to sell to American security firms and government organizations. Putting them on a restricted list is not enough. The democracies and defenders of freedom of the world must unite in an effort to ban the sale of this dangerous spyware program entirely, or if not at the very least to repressive regimes who are prone to use it to illegally monitor and suppress activists.