The NATIONAL INTEREST FOUNDATION

Massive Data Leak Uncovers That Israeli Firm's Spyware Has Been Used to Target Human Rights Activists and Journalists Worldwide

An investigation into a massive data leak revealed that Israeli firm NSO Group's spyware has been used to target human rights activists and journalists worldwide. In total, the probe discovered a list of more than 50,000 phone numbers in over 50 countries that the spyware had accessed. The numbers that were hacked consisted of independent journalists from reputable media entities around the world, politicians, human rights advocates, members of Arab royal families, business executives, and even the top leaders in various nations. The list also included the phone number of Hatice Cengiz, the fiancée of murdered Saudi journalist and dissident Jamal Khashoggi. The media consortium performing the investigation found that a majority of those targeted were in countries with repressive governments that had a history of surveilling their citizens and trying to silence activists. Ultimately, the Israeli spyware has been sold to authoritarian regimes to help them engage in grave violations against their citizenry, and as such, the behavior was strongly condemned by international rights and justice organizations.

The Israeli firm NSO Group developed an advanced cyber spyware called Pegasus for use in compromising and hacking mobile devices of targeted individuals. The military grade technology is sold to authoritarian governments across the world and to nations with a history of surveilling their citizens. NSO Group has refused to identify any of its clients throughout the 40 countries they sell to, and attempted to absolve guilt by claiming them to only consist of intelligence organizations, military personnel, and law enforcement officials – as opposed to repressive regimes – despite evidence refuting this. The spyware is intended to be able to steal as much data as possible, while leaving little trace behind. It is also specifically designed to breach iPhone and Android's security, and be able to take large portions of data and activate the phone's camera and microphone.

The spyware has been used by the NSO Group's clients to spy on its citizens and foreigners within the country. As a result, the loss of confidentiality prevents journalists from connecting with sources, human rights activists from working with citizens abused by the state, and hinders the ability of top national politicians and leaders to work in secure environments. Additionally, the spyware enables repressive governments and agencies to monitor any opposition within a respective country and suppress reporters and critics. When Forbidden Stories and the 17 media organizations began investigating the NSO Group and Pegasus, they uncovered multiple cyberattacks on their reporters as well as their families.

Israel allows the NSO Group to sell its software to malign foreign actors, even outside of the realm of direct criminal investigation. Hence, the use of it to track and violate the rights of non-criminal targets, including those that are trying to expose the abusive behavior of certain government officials and entities. The NSO Group also claims that the spyware cannot be initiated against American systems, but it can still target U.S. citizens overseas using a phone on a foreign network as well. Thus, unsurprisingly, multiple reporters for American and European news outlets have discovered that Pegasus is being deployed against them.