New details show how Pegasus was used to spy on political opponents

Kevin Reed
19 July 2021

Further details emerged on Monday about the nature and extent of the spyware operation called Pegasus that has been used by governments since at least 2016 to hack into the smartphones of thousands of journalists, activists and business and political figures around the world.

The existence of the secret spying software was exposed on Sunday by the French non-profit media group Forbidden Stories and Amnesty International—in cooperation with a reporting consortium that includes the *Guardian*, the *Washington Post* and 15 other media organizations—following a data breach of its developer, the Israeli-based cybersecurity firm NSO, several months ago.

Among the new revelations reported on Monday by the *Guardian* are the fact that at least 50 individuals close to Mexican President Andrés Manuel López Obrador "including his wife, children, aides and doctor" were on the list of possible targets of the Pegasus spyware; Rahul Gandhi, the major political opponent of Indian Prime Minister Narendra Modi, "was twice selected as a potential target in leaked phone number data"; the American daughter of the imprisoned Rwandan activist, Paul Rusesabagina, who inspired the film *Hotel Rwanda*, "has been victim of multiple attacks using NSO spyware."

A report on Monday in the *Washington Post* said that Pegasus is "military-grade spyware" supposedly developed for the purpose of "tracking terrorists and criminals" but it was used on a list of as many as 50,000 cell phone numbers internationally. A forensic investigation conducted by *Post* and the other 16 media partners showed that the NSO spyware successfully infiltrated "37 smartphones belonging to journalists, human rights activists, business executives and two women close to murdered Saudi journalist Jamal Khashoggi…"

While the phone numbers in the leaked NSO data list do not contain the associated names of individuals, reporters have been able to identify "more than 1,000 people spanning more than 50 countries through research and interviews on four continents." Among those identified, the *Post* reports, are "several Arab royal family members, at least 65 business executives, 85 human rights activists, 189 journalists, and more than 600 politicians and government officials—including cabinet ministers, diplomats, and military and security officers. The numbers of several heads of state and prime ministers also appeared on the list."

The journalists targeted in the spying operations work for "CNN, the Associated Press, Voice of America, the New York Times, the Wall Street Journal, Bloomberg News, Le Monde in France, the Financial Times in London and Al Jazeera in Qatar."

The forensic analysis was conducted by Amnesty International's Security Lab on 67 smartphones and, of those, "23 were successfully infected and 14 showed signs of attempted penetration." The testing on the remaining 30 phones was inconclusive.

A *Guardian* report on Monday said that the phone numbers of 15,000 Mexicans were in the leaked data including "Politicians from every party, as well as journalists, lawyers, activists, prosecutors, diplomats, teachers, judges, doctors and academics," and that "cybersurveillance is unregulated and out of control in Mexico—a country where federal and state governments have long used informants, infiltrators and listening devices to monitor and repress dissent."

A report in the *Post* on Monday morning reviewed the manner in which Pegasus infected the iPhone of Claude Mangin, the French wife of a jailed political activist in Morocco. A text message was delivered to

the phone without generating a notification or warning that the iMessage from an unknown sender was skirting Apple's smartphone security and depositing the spyware onto the iPhone.

According to the *Post* report, once Pegasus is on a smartphone, it can "collect emails, call records, social media posts, user passwords, contact lists, pictures, videos, sound recordings and browsing histories," "activate cameras or microphones" and "listen to calls and voice mails." The spyware can "collect location logs of where a user has been and also determine where that user is now, along with data indicating whether the person is stationary or, if moving, in which direction."

In a series of lengthy official statements late Sunday, NSO denied that it was involved in the worldwide government spying operation that has targeted smartphones for the past five years. The company both claimed that the data disclosed by Forbidden Stories and Amnesty International was inaccurate and that it was not responsible the illegal use of its technology by its undisclosed government clients.

In one particularly noteworthy passage, NSO states, "We also stand by our previous statements that our products, sold to vetted foreign governments, cannot be used to conduct cybersurveillance within the United States, and no foreign customer has ever been granted technology that would enable them to access phones with US numbers. It is technologically impossible, and reaffirms the fact that your sources' claims have no merit."

The fact that this statement makes no mention of the US government as a well-known and proven user of similar surveillance tools both domestically and internationally is a transparent admission by NSO that its technology has been approved, if not contracted in the first place, by the American military-intelligence apparatus.

In a series of tweets on Sunday and Monday, the whistleblower and former NSA contractor Edward Snowden denounced NSO and government use of spyware. Responding to the initial reports from the *Guardian* on Sunday, Snowden wrote, "The Israeli company behind this—the NSO group—should bear direct, criminal liability for the deaths and detentions of those targeted by the digital infection vectors it sells, which have no legitimate use."

At noon on Monday, Snowden added, "If we don't do anything to stop the sale of this technology, it's not just going to be 50,000 targets. It's going to be 50 million targets, and it's going to happen much more quickly than any of us expect."

Snowden also wrote, "This is an industry that should not exist: they don't make vaccines—the only thing they sell is the virus," and he also pointed to the fact that the NSO group gave "blood money" to Obama, Trump and Biden officials during their election campaigns.