Report: NSO Group Spyware Found on State Department Phones

govinfosecurity.com/report-nso-group-spyware-found-on-state-department-phones-a-18057

9 US State Department Officials Were Reportedly Hacked Via NSO Software Dan Gunderman (dangun127) • December 3, 2021

Spyware from sanctioned Israeli firm NSO Group has reportedly been detected on at least nine Apple iPhones belonging to U.S. State Department officials with "state.gov" email addresses, who are located in Uganda or whose work focuses on the African nation, according to a Reuters report.

The report - which does not name suspected assailants - cites four people "familiar with the matter" and says the intrusions were detected in the last several months and allegedly represent the most advanced infiltration of NSO Group's software on devices belonging to U.S. officials. Reporting from The Guardian in July linked NSO Group's Pegasus spyware to a list of 50,000 high-profile individuals possibly targeted since 2016, though it is unclear if campaigns were mounted against these individuals.

On the latest developments, a U.S. State Department spokesperson tells Information Security Media Group: "While we are unable to confirm, generally speaking the department takes seriously its responsibility to safeguard its information and continuously takes steps to ensure information is protected."

An NSO Group spokesperson tells ISMG: "Once the inquiry was received, and before any investigation under our compliance policy, we have decided to immediately terminate relevant customers' access to the system, due to the severity of the allegations.

"To this point, we haven't received any information, nor the phone numbers, nor any indication that NSO's tools were used in this case," the spokesperson said. "On top of the independent investigation, NSO will cooperate with any relevant government authority and present the full information we will have."

The company has maintained that it sells its Pegasus spyware to clients who use it for legitimate law enforcement purposes and not for active surveillance.

The NSO Group spokesperson said: "To clarify, the installation of our software by the customer occurs via phone numbers. As stated before, NSO's technologies are blocked from working on US (+1) numbers. Once the software is sold to the licensed customer, NSO has no way to know who the targets of the customers are. As such, we were not and could not have been aware of this case."

Americans using devices with foreign phone numbers remain vulnerable, however, according to recent reporting.

Target: Misuse of Repressive Tools

The U.S. State Department representative said: "As part of its commitment to put human rights at the center of U.S. foreign policy, the Biden-Harris administration is taking action to stem the proliferation and misuse of digital tools used for repression."

The spokesperson also highlighted the U.S. Department of Commerce's effective blacklisting of NSO Group and Candiru, after "investigative information [showed] that these companies developed and supplied spyware to foreign governments that used these tools to maliciously target government officials, journalists, businesspeople, activists and academics."

Sanctions against the Israeli company came via a final rule from the Commerce Department's Bureau of Industry and Security, or BIS, which said that the companies "threatened the privacy and security of individuals and organizations worldwide." Those on the Entity List cannot purchase U.S. technologies or goods without a license provided by the Department of Commerce.

At the time, the State Department confirmed that it would not be "taking action against countries or governments where these entities are located."

To sell the product internationally, the Israeli Ministry of Defense must approve NSO export licenses.

A spokesperson for the Israeli embassy to the U.S. tells ISMG of the latest news: "Israel hasn't received any official inquiry on this matter. If and when one is received, it will be investigated. Cyber products like the one mentioned are supervised and licensed to be exported to governments only for purposes related to counterterrorism and severe crimes. The licensing provisions are very clear and if these claims are true, it is a severe violation of these provisions."

Rick Holland, a former intelligence analyst for the U.S. Army who's now the CISO for security firm Digital Shadows, tells ISMG, "There is increasing private sector (e.g., Apple), and now U.S. government (e.g., Commerce Department) pressure against Israel to curb the NSO Group's activities. These are just one hot spot in U.S.-Israeli relations, but don't prioritize when weighed against other policy areas like Iran. NSO Group will likely continue to operate as they have in the past."

(Photo: jorono/1035 images via Pixabay)

NSO Seeks Reversal

An NSO spokesperson told The Hill last month that the firm was dismayed by the decision to be placed on the Entity List, saying its technologies "support U.S. national security interests and policies by preventing terrorism and crime. ... Thus, we will advocate for this decision to be reversed."

Facebook's WhatsApp previously sued NSO Group, accusing it of using WhatsApp to target some 1,400 officials in nearly two dozen countries. In September, Apple issued emergency updates for its products after discovering a graphics processing vulnerability that left them susceptible to NSO Group spyware.

The French government reportedly pulled out of a deal with NSO Group after accusations surfaced that its spyware was being used by an NSO customer to target French President Emmanuel Macron (see: *Report: Israel Cuts Cyber Export List to 37 Countries*).

New Lawsuit, Updated Export List

Late last month, Apple sued NSO, alleging that the spyware maker abused Apple's products and services to carry out spying operations without the consent of the company or its users.

The Israeli Ministry of Defense has reportedly reduced the number of countries to which Israeli companies' cyber spyware can be exported from 102 to 37. The government's list restricts cyber spyware companies in Israel from doing business with countries that were previously customers, such as Morocco, Mexico, Saudi Arabia and the United Arab Emirates.

The list restricts companies from doing business with anyone involved in offensive cyber operations, countries where there are totalitarian regimes or countries where there are suspicions of a violation of civil rights, according to a report by Israeli outlet Calcalist.