US State Dept employees’ phones hacked using NSO spyware

By Sergiu Gatlan

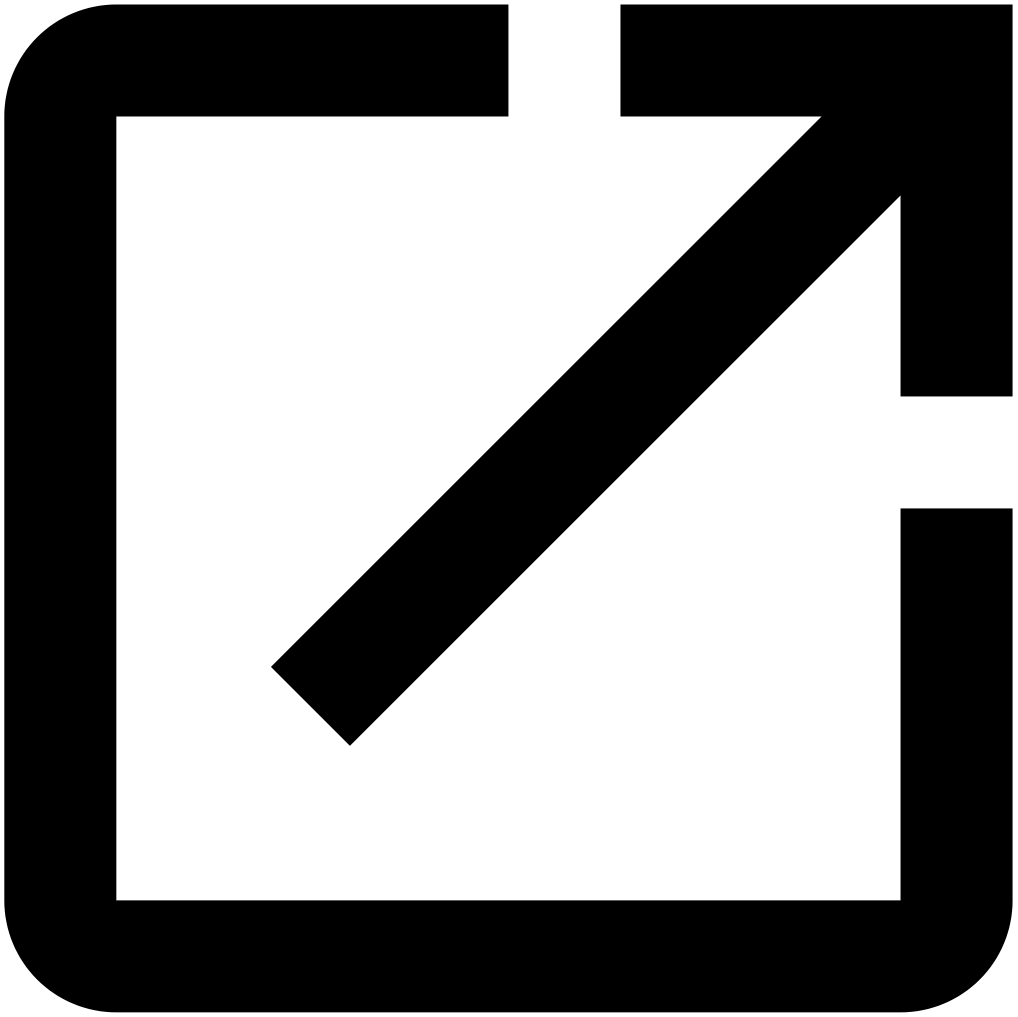
Published: 2021-12-03 · Archived: 2026-04-05 15:02:59 UTC

Apple has warned US Department of State employees that their iPhones have been hacked by unknown attackers using an iOS exploit dubbed ForcedEntry to deploy Pegasus spyware developed by Israeli surveillance firm NSO Group.

The attacks hit US officials (at least 11 according to the Washington Post) based in or focused on matters concerning the East African country of Uganda and took place in recent months, according to anonymous sources cited by Reuters today.

While NSO canceled the customer accounts behind these intrusions and promised to investigate the attacks, a spokesperson told Reuters—who first reported the attacks—that the company doesn't know what tools were used in the attack. NSO also declined to name the suspended customers.


DIE LINKE.
0:00



"On top of the independent investigation, NSO will cooperate with any relevant government authority and present the full information we will have," an NSO spokesperson separately told Motherboard.

"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."

The news of Department of State employees' phones being hacked to install Pegasus spyware comes on the heels of the US sanctioning NSO Group and three other companies from Israel, Russia, and Singapore last month for spyware development and selling hacking tools used by state-sponsored hacking groups.

NSO and Candiru have been added to the Commerce Department's Bureau of Industry and Security (BIS) Entity List for supplying the software used by state hackers to spy on government officials, journalists, and activists.

Positive Technologies from Russia and Computer Security Initiative Consultancy PTE. LTD. from Singapore were sanctioned for the trafficking of exploits and hacking tools.

"Specifically, investigative information has shown that the Israeli companies NSO and Candiru developed and supplied spyware to foreign governments that used this tool to maliciously target government officials, journalists, businesspeople, activists, academics, and embassy workers," reads the Department of Commerce's final ruling.

In early November, Apple has also filed a lawsuit against NSO and its parent company for targeting and spying on Apple users with surveillance tech.

For instance, NSO's ForcedEntry exploit (also used to hack the nine State Dept employees) was employed by state attackers to compromise Apple devices and install Pegasus spyware, as revealed by the Citizen Lab in August.

Apple added at the time that it will notify all users targeted using the ForcedEntry exploit (alerts that were also sent to the hacked State Dept employees) and those who will be targeted in state-sponsored spyware attacks in the future, "in accordance with industry best practices."

Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.
