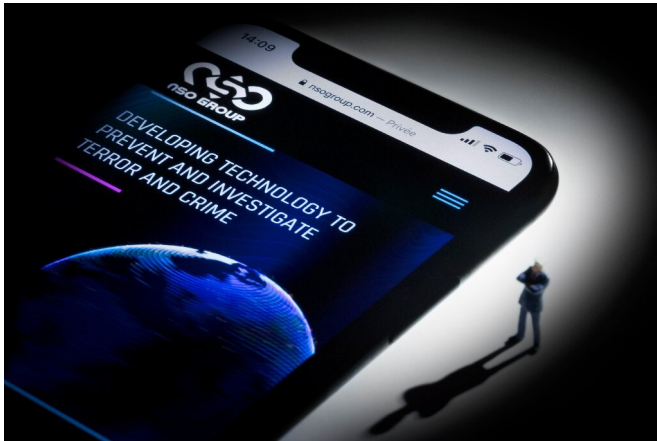


Pegasus maker probes reports its spyware targeted US diplomats

4 December 2021



The Israeli spyware maker NSO says it is probing reports it technology was used to target US diplomats in Africa.

The Israeli spyware maker in the Pegasus surveillance scandal said Friday it was investigating reports the firm's technology was used to target iPhones of some US diplomats in Africa.

Apple has begun alerting people whose phones were hacked by NSO's spyware, which essentially turns handsets into pocket spying devices and sparked controversy this year after reportedly being used on activists, journalists and politicians.

"On top of the independent investigation, NSO will cooperate with any relevant government authority and present the full information we will have," the firm said in a statement.

NSO said it has not confirmed its tools were used, but opted to "terminate relevant customers' access to the system" due to the seriousness of the allegations reported by Reuters and the Washington Post.

The Post reported that Apple alerted 11 US diplomats that their iPhones were hacked in recent months, citing people familiar with the notifications who said the attacks focused on officials working in Uganda or east Africa.

NSO Group's spyware has been engulfed in scandal since reports that Pegasus was used by foreign government clients to target the phones of human rights activists, embassy employees and others.

Apple sued the firm last month seeking to block NSO from using the Silicon Valley giant's services to target the over one billion iPhones in circulation.

Reuters, citing four people familiar with the matter, said nine American diplomats were targeted and added the intrusions represented the widest known hacks of US officials using NSO technology.

Apple declined to comment on the reports.

Just weeks before the Apple lawsuit, US authorities blacklisted NSO to restrict exports from American groups over allegations the Israeli firm "enabled foreign governments to conduct transnational repression."

Smartphones infected with Pegasus are essentially turned into surveillance devices, allowing the user to read the target's messages, look through their photos, track their location and even turn on their camera without them knowing.

Concern over Pegasus spyware further grew after Apple revealed in September it had patched a weakness that allowed NSO's [spyware](#) to infect devices without users even clicking on a malicious message or link.

The so-called "zero-click" attack is able to silently corrupt the targeted device, and was identified by researchers at Citizen Lab, a cybersecurity

watchdog organization in Canada.

Apple said at the time it filed the lawsuit in a California federal court that it would notify the "small number" of users that it discovered may have been targeted by those types of attacks.

© 2021 AFP

APA citation: Pegasus maker probes reports its spyware targeted US diplomats (2021, December 4) retrieved 20 May 2022 from <https://techxplore.com/news/2021-12-pegasus-maker-probes-spyware-diplomats.html>

This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.