US blacklists Israeli maker of Pegasus spyware

November 3 2021, by Joshua Melvin

Smartphones infected with Pegasus are essentially turned into pocket spying 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.

US authorities on Wednesday put the Israeli maker of the Pegasus

spyware at the center of a scandal over surveillance of journalists and officials on a blacklist of restricted companies.

The company, NSO, was engulfed in controversy over reports that tens of thousands of human rights activists, journalists, politicians and business executives worldwide were listed as potential targets of its Pegasus software.

Smartphones infected with Pegasus are essentially turned into pocket spying 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.

"These tools have... enabled foreign governments to conduct transnational repression, which is the practice of authoritarian governments targeting dissidents, journalists and activists outside of their sovereign borders to silence dissent," the US Commerce Department said in a statement.

NSO fired back at the decision, saying its "technologies support US national security interests and policies by preventing terrorism and crime."

"We will advocate for this decision to be reversed," a NSO spokesperson told AFP, adding its compliance controls have resulted in "multiple terminations of contacts with government agencies that misused our products."

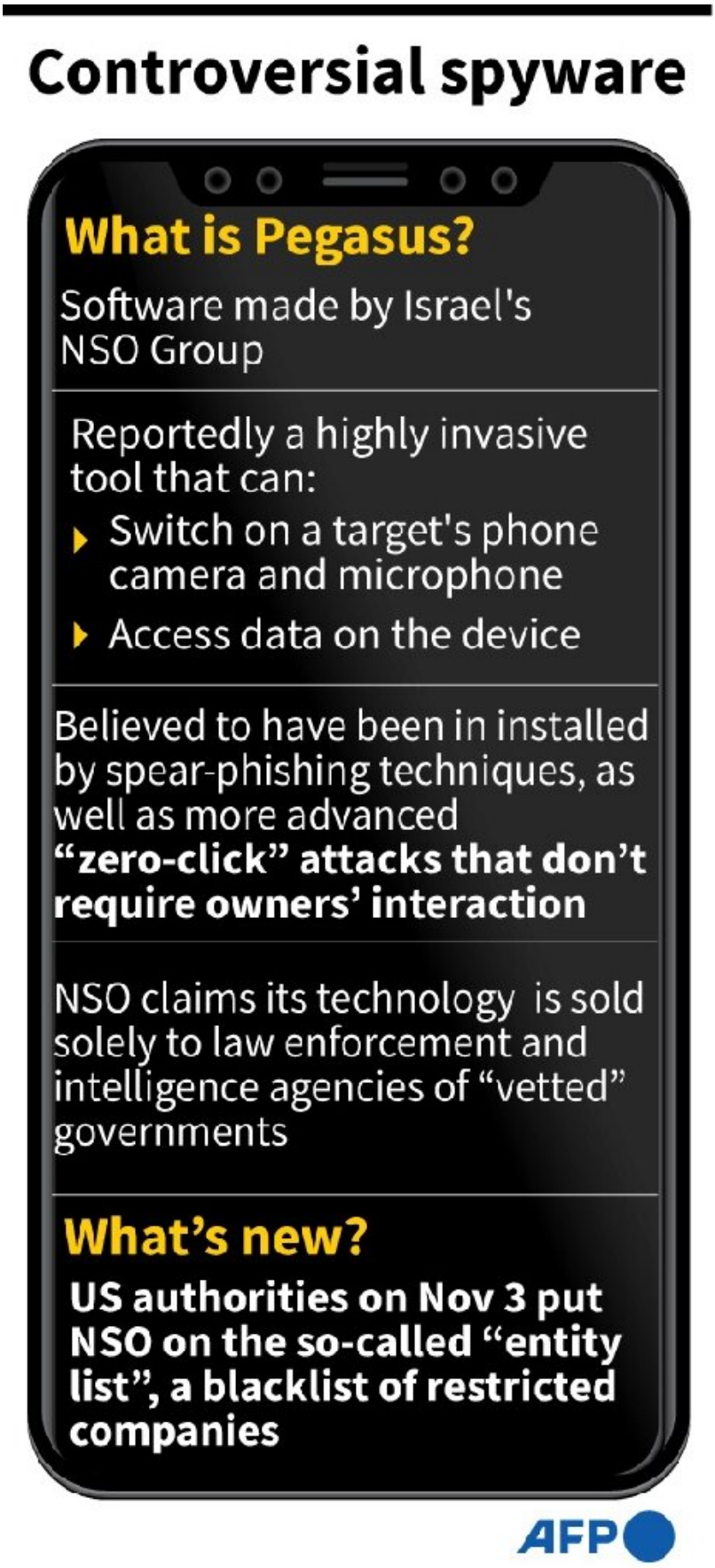
Washington also targeted Israeli company Candiru, as well as Singapore-based Computer Security Initiative Consultancy PTE (COSEINC) and Russian firm Positive Technologies that were accused of trafficking in hacking tools.

The companies' addition to the so-called "entity list" means exports to them from US organizations are restricted—and it is now far harder for American researchers to sell them information or technology.

In a statement, Positive Technologies said the listing would have "little or no effect on our business" and did not come as a surprise.

"We sincerely believe that geopolitics should not be an obstacle to the technological development of society, and we will continue to do what we do best – to ensure cybersecurity on a global scale," it said on its website.

COSEINC did not respond to a request for comment from AFP.


Controversial spyware
What is Pegasus?
Software made by Israel's NSO Group
Reportedly a highly invasive tool that can:
Switch on a target's phone camera and microphone
Access data on the device
Believed to have been in installed by spear-phishing techniques, as well as more advanced "zero-click" attacks that don't require owners' interaction
NSO claims its technology is sold solely to law enforcement and intelligence agencies of "vetted" governments
What's new?
US authorities on Nov 3 put NSO on the so-called "entity list", a blacklist of restricted companies
AFP

Background factfile on the Pegasus spyware developed by Israeli software firm NSO Group.

'Zero-click' attack

Critics say the widespread availability of software like Pegasus now allows even cash-strapped authoritarian governments to effectively acquire their own highly invasive surveillance powers.

"NSO Group's spyware is a tool of repression, which has been used around the world to violate human rights," Danna Ingleton, deputy director of Amnesty Tech, said in a statement.

"This dangerous industry is out of control, and this must spell the end of the impunity spyware companies have so far enjoyed," Ingleton added.

A key problem is that companies that supply spyware are left to judge what is an appropriate use of their technology and whether buyers can be trusted to honor restrictions.

"It's pretty clear that most governments ignore those constraints and do what they believe to be in (their) self-interest," said Oliver Tavakoli, chief technology officer at cybersecurity company Vectra.

UN experts have called for an international moratorium on the sale of surveillance technology until regulations are implemented to protect human rights following the Pegasus scandal.

Following the initial concern over Pegasus, a subsequent wave of worries

emerged when iPhone maker Apple released a fix in September for a weakness that can allow the spyware to infect devices without users even clicking on a malicious message or link.

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