

Biden's executive order limits government's use of commercial spyware

Getty Images

reader comments

23 with

Share this story

President Joe Biden on Monday signed an executive order barring many uses by the federal government of commercial spyware, which has been increasingly used by other countries in recent years to surveil dissidents, journalists, and politicians.

The signing of the executive order came as administration officials told journalists that roughly 50 US government personnel in at least 10 countries had been infected or targeted by such spyware, a larger number than previously known. The officials didn't elaborate.

Commercial spyware is sold by a host of companies, with the best known being NSO Group of Israel. The company sells a hacking tool known as Pegasus that can surreptitiously compromise both iPhones and Android devices using "clickless" exploits, meaning they require no user interaction. By sending a text or ringing the device, Pegasus can install spying software that steals contacts, messages, geo locations, and more, even when the text or call isn't answered. Other companies selling commercial spyware include Cytox, Candiru,

and Paragon.

While NSO describes Pegasus as a “lawful intercept” tool that’s sold only to legitimate law-enforcement agencies to investigate crime and terrorism. Mexico, India, Saudi Arabia, the United Arab Emirates, Morocco, and other countries have been caught deploying it against political dissidents, journalists, and other citizens that aren’t accused of any crimes. In November 2021, the Biden administration restricted the export, re-export, and in-country transfer of products from NSO and three other companies in Israel, Russia, and Singapore.

Monday’s executive order goes further by barring federal agencies, including those engaged in law enforcement, defense, or intelligence activities, from “operationally using” commercial spyware.

Advertisement

“The proliferation of commercial spyware poses distinct and growing counterintelligence and security risks to the United States, including to the safety and security of US Government personnel and their families,” a fact sheet published by the White House said. “US Government personnel overseas have been targeted by commercial spyware, and untrustworthy commercial vendors and tools can present significant risks to the security and integrity of US Government information and information systems.”

White House officials aren’t naming the specific spyware that’s barred, but using the term commercial spyware strongly implies it includes tools sold by NSO, Cytrox, Candiru, and others. Criteria for tools falling under the order include if:

- they’re abused by a foreign government in an attempt to access the device of a US citizen
- a foreign actor deploys them against activists or dissidents in an attempt to intimidate or curb dissent or opposition or squelch expressions of free speech

- they're supplied to governments for which there are credible reports that they engage in systematic acts of political repression.

The officials declined to say if US law enforcement and intelligence agencies currently use commercial spyware. Last year, the FBI confirmed a New York Times report that the bureau had bought NSO Group's Pegasus tool for product testing and evaluation but said they weren't used for operational purposes or to support any investigation. The US Drug Enforcement Agency, the NYT has also reported, deployed a surveillance tool called Graphite for use in counternarcotics operations.

<https://arstechnica.com/?p=1927199>