A Hacked Newsroom Brings a Spyware Maker to U.S. Court | The New Yorker

By Ronan Farrow
January 17, 2023

NSO Group's business is founded on secrecy; it has refused to publicly identify its clients. In the statement, the company said it sells its software only to "legitimate government agencies" for use in state intelligence and law-enforcement efforts, and maintained that its tools "have proven to save thousands of lives around the world." It claimed that the firm "cannot know who the targets of its customers are." Yet it cites its own "rigorous and unique compliance policies" and says it has "terminated contracts when misuse was found."

Many of the Salvadoran journalists who were hacked told me that they believe that whoever deployed Pegasus against them is connected to the Bukele regime. Citizen Lab said that its findings point to the existence of an NSO client operating Pegasus in El Salvador, and reporters were often hacked as they worked on stories of importance to the Bukele regime. "We analyzed the exact time line," Herrero, the Access Now investigator, recalled. "If somebody was reporting on corruption, then, boom, they got hacked seven days a week." Carlos Martínez, an El Faro reporter and the brother of Óscar Martínez, the executive editor, told me, "It's very clear for us that the Bukele government is trying to stop us, to stop our job and to destroy us as individuals and as an organization."

[…]

Source: A Hacked Newsroom Brings a Spyware Maker to U.S. Court | The New Yorker