Critics of Serbia’s government targeted with ‘military-grade spyware’

Publication Date: 2023-11-28

Author: Stephanie Kirchgaessner

Section: Technology

Tags: Hacking, Serbia, Europe, news

Article URL: https://www.theguardian.com/technology/2023/nov/28/critics-of-serbias-government-targeted-with-military-grade-spyware

Critics of Serbia’s nationalist government who have documented the country’s endemic corruption were targeted with military-grade spyware earlier this year, according to new findings by security researchers. The attempted hacking of two Serbian pro-democracy activists – who have asked not to be named to protect their safety – was ultimately not successful because both individuals’ Apple iPhones had been updated with the latest iOS software, which the researchers said protected the devices from being infiltrated. The individuals were first alerted of the attempted hack by Apple, which sent both an alert that they may have been targeted by a state-sponsored actor. The warning was later confirmed after investigations by researchers at Access Now, the Share Foundation in Serbia, the Citizen Lab at the Munk School at the University of Toronto, and Amnesty International. The findings come just months after researchers revealed that Russian journalists who are critical of Vladamir Putin and living in the European Union had also been targeted with spyware. The Council of Europe and the European parliament have sought to advance policies that would curb the use of spyware, but the emergence of new cases inside the bloc point to an apparent willingness by some European governments to continue to use spyware to suppress and intimidate political critics. Natalia Krapiva, the tech-legal counsel at Access Now, said: “These findings are extremely worrying for the rule of law and democracy in Serbia. Uncontrolled use of commercial spyware is poison not only for human rights, but also security and democratic institutions in any country.” The researchers found that the Serbians had been targeted about a minute apart from each other on or about 16 August 2023. Access Now and Citizen Lab discovered traces of the attempted attack, which sought to take advantage of a possible vulnerability in iPhone’s HomeKit application. The researchers said use of the technical vulnerability was “consistent” with those previously used by states improperly using one of the world’s most sophisticated cyber weapons, known as Pegasus, which is sold by Israel’s NSO Group. When Pegasus is successfully deployed against a target, it can essentially take over a mobile phone, including turning the phone into a portable listening device. It can also access information held in encrypted applications and view a user’s photographs and messages. The researchers in the Serbian case could not definitively confirm what kind of spyware was used because available forensic indicators were limited. “We aren’t attributing these attacks to a particular operator at this time, but we note that a decade of Citizen Lab investigations have found that Serbia is a regular customer for mercenary spyware and other commercial surveillance technologies,” said John Scott-Railton, a senior researcher at Citizen Lab. NSO said in a statement to the Guardian that Citizen Lab and Access Now’s report were “inconclusive”. The company has repeatedly said that Pegasus is sold to governments for the purpose of being used in serious crime and terror investigations and

that its use “saves lives”. It added: “NSO does not operate its technology and is not privy to the collected intelligence.” While the researchers could not definitively attribute the attempted attacks in Serbia to a specific spyware, the attempted hacks are likely to renew focus on past findings involving covert data collection and surveillance by Serbia’s Security Information Agency (BIA). The BIA’s most recent director was Aleksander Vulin, who was placed on a sanctions list by the US Treasury in July 2023 for his support of Moscow and for using “his political positions to build support for Russia’s malign activities” and fuel instability in Serbia. Vulin resigned from his position on 3 November. One alleged victim of the hacking attempt who was interviewed by the Guardian described their work as focused on being critical of Serbia’s “autocratic regime” and the country’s “widespread corruption”, as well as the current government’s pro-Russian foreign policy, which has not aligned with the EU on issues such as sanctions against Moscow. The attempted hacking, the person said, was likely an attempt to intimidate or discredit their work, “to find something compromising against me”. Both of the individuals who were targeted believed the attempted hacks could also have been connected to calls for official inquiries into the government’s handling of a mass shooting that left 17 people – including children – dead last summer. Mass demonstrations erupted in the wake of the shooting, with protesters decrying the populist president Aleksandar Vučić, who was blamed for creating divisions within the country that some alleged led to the mass shooting. The Serbian government did not respond to requests for comment.