Serbia: BIRN journalists targeted with Pegasus spyware

Published: 2025-03-27 · Archived: 2026-04-05 18:40:49 UTC

Two journalists from Balkan Investigative Reporting Network (BIRN), an award-winning Serbian network of investigative journalists, were targeted with NSO Group's Pegasus spyware last month, a new Amnesty International investigation reveals.

Journalists Bogdana (not her real name) and Jelena Veljkovic received suspicious messages on the Viber messaging app from an unknown Serbian number linked to Telekom Srbija, the state-telecommunications operator.

Suspecting that their smartphones were being targeted by a spyware attack, they approached Amnesty International's Security Lab, whose forensic analysis confirmed their suspicions.

> "We discovered that the text messages contained hyperlinks to a Serbian language domain name which we have determined with high confidence to be associated with NSO Group's Pegasus spyware,
>
> *Donncha Ó Cearbhaill, the Head of Amnesty International's Security Lab.*

This is the third time in two years that Amnesty International's Security Lab has found NSO Group's Pegasus spyware being used against civil society in Serbia. In November 2023, Amnesty International, Access Now, SHARE Foundation and Citizen Lab documented how two Serbian civil society members where targeted by a zero-click spyware attack, which Amnesty International later attributed as Pegasus attack attempts.

On 14 February 2025, Bogdana received a message on Viber with a link to a news article and a message asking: "Do you have info that he is next? I heard something completely different."

At the time she was working on an article about foreign investments and state-linked corruption cases. The previous day she had met sources for her story including individuals close to the government.

Bogdana did not click the Pegasus infection link, and a forensic analysis of her device did not indicate that Pegasus spyware had been installed on her phone. Amnesty International's Security Lab later found that, if clicked, the infection link redirected to a decoy page on a Serbian media website, a technique previously seen in a Pegasus attempt targeting a Serbian protest leader in July 2023.

NSO Group stated in a letter to Amnesty International that "all sales of our systems are to vetted government end-users". Amnesty International believes that the continued use of Serbian language Pegasus infection domain names, and the targeting of Serbian civil society with a consistent methodology are indicative of these attacks being carried out by a Serbian state entity.

Bogdana said: "When I found out that the link on my phone was Pegasus, I was absolutely furious. This was the phone registered to my name, and I felt as if I had an intruder in my own home. This is an unnerving feeling…. I was extremely concerned about my sources who could be at risk because they communicated with me."

Jelena Veljkovic received a similar Viber message to the one sent to Bogdana from the same Serbian phone number on 14 February and deleted it without clicking it. Amnesty International concluded that, based on the nature of the attempt, this was also a Pegasus 1-click infection attempt. 1-click attacks require action from the target to enable the infection of their device, typically the opening of a malicious link.

“When I found out that I was a target of a Pegasus attack, I was not particularly scared but found it quite unsettling. This was my private telephone, which I also use for work, and a virus like Pegasus, which is not selective at all and can access everything on one’s phone, can have repercussions on my family too.

> “This was a targeted attack on investigative journalists – a form of pressure and a warning. Whether it was an attack on me personally or on BIRN, as a media outlet, I am not sure,
>
> *Jelena.*

BIRN and its staff face frequent threats, harassment and Strategic Lawsuits against Public Participation (SLAPPs), including by senior government officials, for their investigative journalism. Currently it is fighting four SLAPP suits, mostly filed by public officials, including the current mayor of Belgrade, or others with known links to the authorities.

Amnesty International shared its findings with NSO Group who responded saying: “We cannot comment on specific existing or past customers. Additionally, as a matter of policy, we are unable to disclose any information regarding our technical specifications, functionality or operational features of our products.”

Repeated attempts to engage the Serbian Security Information Agency (BIA, Bezbednosno-informativna Agencija) were unanswered.

These findings provide further evidence that Serbian authorities are abusing highly invasive spyware products and other digital surveillance technologies to target journalists, activists, and other members of civil society amid widespread student protests that have gripped the country since November 2024.

Serbian authorities must **stop using highly invasive spyware** and provide effective remedy to victims of unlawful targeted surveillance and hold those responsible for the violations to account. NSO Group must stop selling Pegasus and the use of its products in Serbia.
