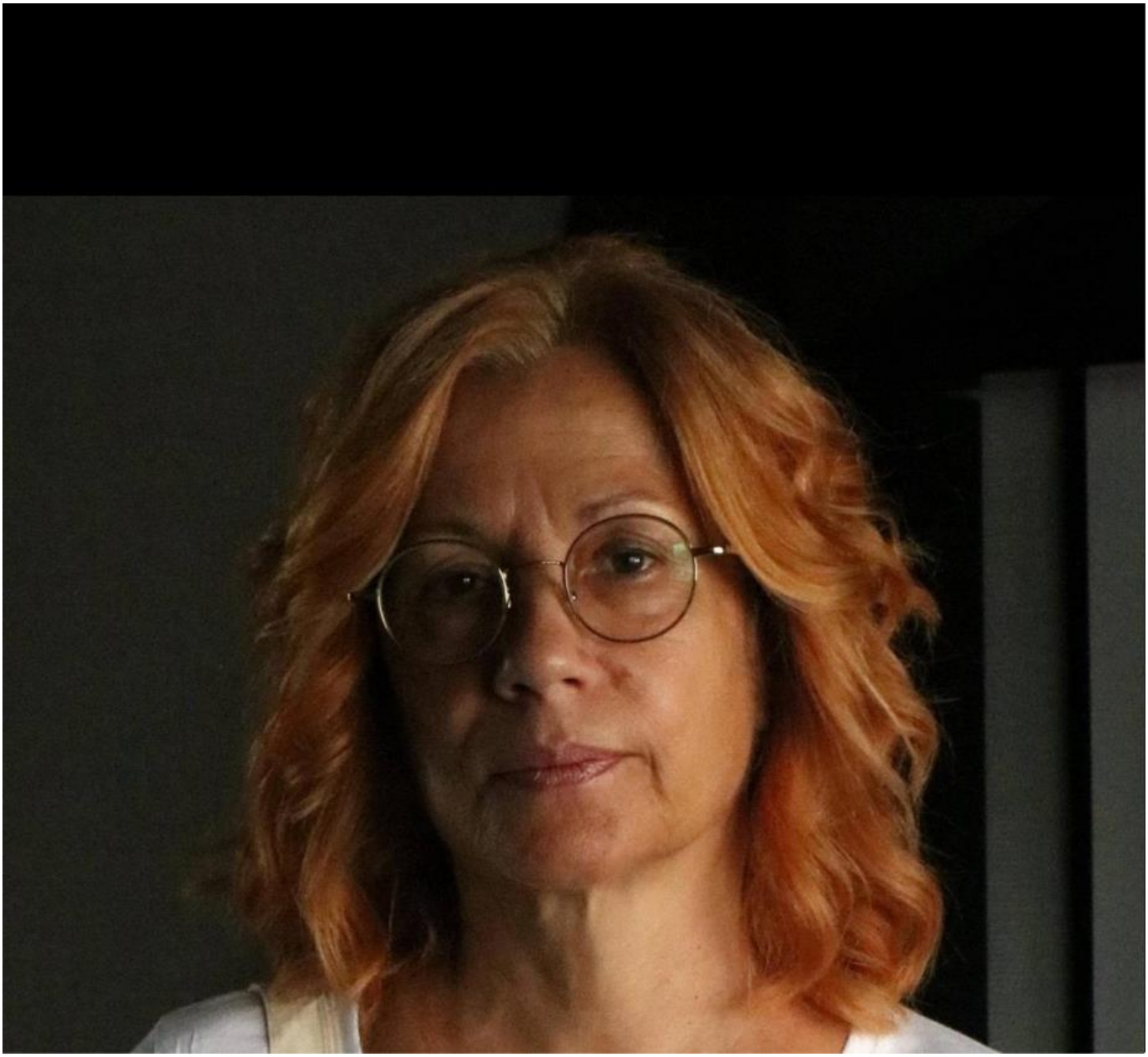

JOURNALISTS TARGETED WITH PEGASUS SPYWARE

TECHNICAL BRIEFING

AMNESTY INTERNATIONAL

CONTENTS

Cover photo: Jelena Veljković, one of the journalists targeted with Pegasus spyware.

This technical briefing documents how two journalists in Serbia were targeted with NSO Group's Pegasus spyware in February 2025. The briefing builds on the evidence of a widespread surveillance campaign against Serbian civil society that we documented in our 2024 report "A Digital Prison".

INTRODUCTION

Amnesty International has found evidence that two journalists at the Serbia-based Balkan Investigative Reporting Network ("BIRN"), an award-winning network of investigative journalists, were targeted with NSO Group's Pegasus spyware in February 2025.

These new findings of ongoing Pegasus targeting further strengthen 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 in the country. This evidence builds on Amnesty International's December 2024, "A Digital Prison" report, which documented the systematic and unlawful targeting of civil society in Serbia with mobile forensic technology developed by Cellebrite and three forms of spyware, including Pegasus and a domestically-developed Android spyware system. BIRN was Amnesty International's investigative partner in the "A Digital Prison" investigation.

This is the third time in two years that Amnesty International's Security Lab has found NSO Group's Pegasus being used against civil society in Serbia. In November 2023, Amnesty International and its partners Access Now, SHARE Foundation and Citizen Lab documented how two Serbian civil society members were targeted by a zero-click spyware attack. In "A Digital Prison", Amnesty International attributed the two earlier cases of zero-click targeting to NSO Group's Pegasus spyware. The research also revealed a previously unreported third case in which a Serbian activist was targeted with a Pegasus 1-click infection link back in July 2023.

Amnesty International wrote to NSO Group on 14 March 2025 to present these latest findings. On 18 March 2025, NSO Group replied to state that "As stated in the past, we reiterate 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. Furthermore, NSO Group is closely regulated by export control authorities in the countries from which we export our products. Our commitment to maintain the highest standard of ethical conduct as well as confidentiality towards our customers is paramount and is consistent with industry norms and our legal obligations". NSO Group also stated that it "takes seriously its responsibility to respect human rights and is fully committed to upholding the UN Guiding Principles on Business and Human Rights (UNGPs)".

JOURNALISTS IN SERBIA UNDER ATTACK

The two journalists targeted with Pegasus spyware in February 2025 work for BIRN, whose journalists and editors have faced frequent threats, harassment and Strategic Lawsuits against Public Participation (SLAPPs), including by senior government officials, for their investigative journalism. Independent media in Serbia generally operate in a highly challenging environment. Journalists investigating organized crime, corruption and their links with the authorities are often subjected to smear campaigns, serious online abuse and physical attacks, as well as baseless financial investigations. At the time of writing, BIRN alone is fighting four SLAPP suits, filed by public officials, including the current mayor of Belgrade, or businesspeople with known links to the authorities.

The journalists received suspicious messages on the Viber messaging app from an unknown phone number. Both Viber messages were sent by the same Serbian phone number, +381659940263, which is assigned to Telekom Srbija, a Serbian state-owned telecommunications operator. After suspecting that these Viber messages were an attempt to install spyware on their phones, the journalists reached out to Amnesty International's Security Lab for support.

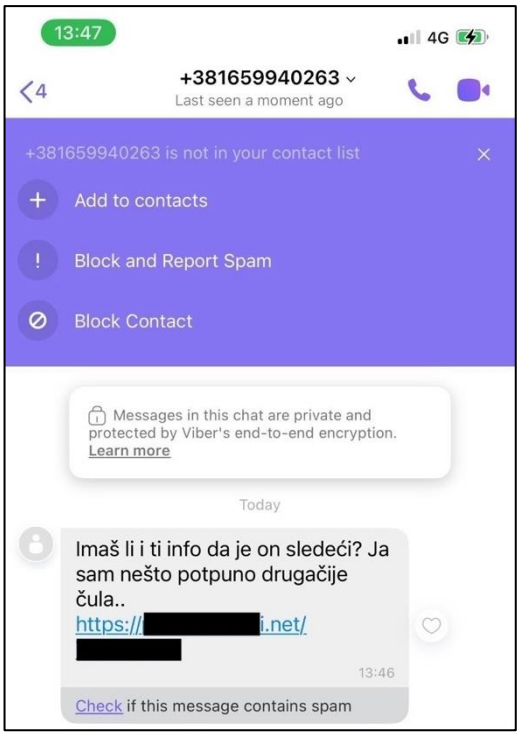

Figure 1: Screenshot of a Viber message received by "Bogdana" on her iPhone on 14 February 2025 at 13:46 local time.

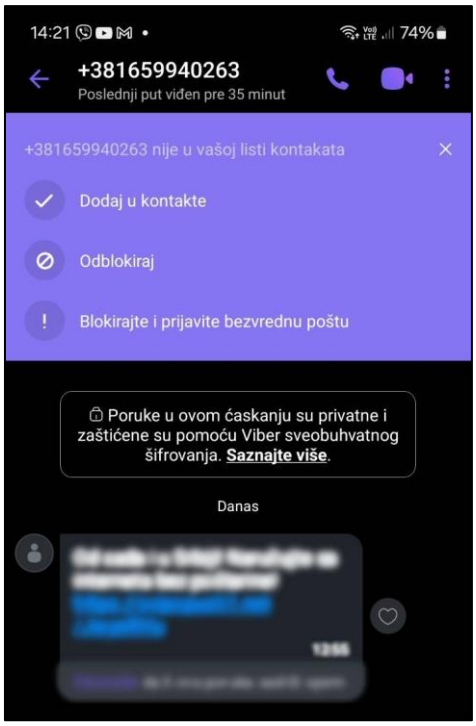

Figure 2: Screenshot of a Viber message received by "Bo Jelena Veljković on her Android phone at around 12:55 local time in Serbia, also on 14 February

CASE 1: "BOGDANA" - PEGASUS INFECTION LINK SENT TO IPHONE

"Bogdana", who wishes to remain anonymous for security reasons and in order to protect the confidentiality and security of her sources, is a highly regarded senior investigative journalist with BIRN. For many years, her research focused on uncovering links between organized crime gangs and government officials and state-sponsored corruption. In her research, she heavily relies on documents and credible, yet extremely sensitive, sources.

On 14 February 2025, "Bogdana" received a suspicious message from an unknown number on the Viber messaging app. The message, written in an informal tone, read "Do you have info that he is next? I heard something completely different," and included a link to a news article.

At the time, "Bogdana" was working on an article about foreign investments in an industry sector and state-sponsored corruption in Serbia and had only a day earlier met with important sources for the story, including individuals close to the government. Although she thought that the cryptic message may have made a vague reference to her source and was tempted to open it, she knew better than to click on the link.

Amnesty International's forensic analysis of "Bogdana's" phone and the suspicious messages determined with high confidence that the link included was an attempt to install the Pegasus spyware.

"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,"

"Bogdana" told Amnesty International. As other journalists targeted with invasive spyware, her prime concern was about the confidentiality and safety of her sources.

"I wasn't extremely worried that they could have used some of my personal information they accessed to potentially compromise me, but I was extremely concerned about my sources that could be at risk because they communicated with me."

"Bogdana" was not particularly surprised with the attempted attack and reflected on an already challenging environment for media in Serbia. "The context in which independent media in Serbia operate is completely volatile. When we investigate and write about an issue, we never know which bit of information and detail will irritate someone, but we can all expect retribution sooner or later."

What did take her aback, however, was the type of digital attack. Pegasus spyware is notoriously expensive for use and governments across the world reserve it for high-value targets. "In Serbia, you can hire a hitman for a half of the money! If they are willing to pay this much money to tap my phone, what else would they be prepared to pay for?!"

"Threats, harassment, surveillance – they have already tried everything. They behave as if there is no rule of law. In any other normal state, even one of my stories would have shaken the very existence of the government. Here, we produce the whole series and nothing happens."

ANALYSIS OF ATTACK MESSAGE

"Bogdana" received a Viber message on her iPhone on 14 February 2025 at 13:46 local time. The message was sent from a Viber account registered with the phone number +381659940263.

The screenshot (see Figure 1) includes text in Serbian and a hyperlink to a Serbian language domain name. The original message included a random 8-character URL which Amnesty International has redacted.

Amnesty International has determined with high confidence that the domain contained in the link is associated with NSO Group's Pegasus spyware. The determination was based on evidence gathered by Amnesty International as part of our multi-year investigation into the misuse of NSO Group's Pegasus spyware and other forms of highly invasive spyware which poses a risk to civil society.

"Bogdana" did not click the link, and there was no indication that the Pegasus spyware was successfully installed on the phone.

When opened by Amnesty International investigators in a secure environment, the Pegasus infection link redirected to a decoy page at https://n1info.com, another Serbian media website. We note that a previous Pegasus 1-click attack attempt targeting a Serbian protest leader in July 2023 also redirected to the same media website (see "A Digital Prison" report).

We believe the continued use of n1info.com as a decoy domain for expired or failed Pegasus infection links, alongside the use of a Serbian language domain name, is indicative of the attacks being carried out by a single Serbian Pegasus customer who is using a consistent and repeated attack methodology.

CASE 2: JELENA VELJKOVIĆ: PEGASUS INFECTION LINK SENT TO ANDROID

The second BIRN individual targeted in this campaign was Jelena Veljković, an award-winning journalist whose investigations focus on politics, public finance, corruption and war crimes. Most recently, Jelena has been researching the links between high-profile corruption cases and individuals close to the government. Jelena too received a message with an infection link from the same phone number on 14 February 2025.

Originally, Jelena did not think that the message was suspicious, but she found it strange that it was showing as a blurred message on her telephone screen. Only when she found out that one of her colleagues received the same message the same day, she became concerned.

"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."

For Jelena, the message of an attack like this was clear. "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. What I do know is that this attempted attack has caused a great deal of consternation among all colleagues in our media room," Jelena told Amnesty International.

Jelena says that the attack only made her even more careful when dealing with sensitive sources and communicating via telephone. "I now opt for personal communication and direct meetings over the convenience of telephone communication, which has only made the logistics of interviews more complicated, and the entire process takes more time, but I don't think I have an alternative. What is particularly frustrating is that there is no certain way to protect yourself against these types of digital attacks – Pegasus does not necessarily require one to click on a malicious link to get their phone infected. No precautions and measures will keep you safe."

ANALYSIS

Jelena received a message with an infection link over Viber around 12:55 local time in Serbia, also on 14 February (see Figure 2).

The attack message was sent from the same Serbian phone number, +381659940263, used to target her colleague. Jelena deleted the suspicious message shortly after receiving it. As the message request was not accepted, it was not possible to determine the full URL included in the message.
While it was not possible to recover the original link, Amnesty International concludes that this was also a Pegasus 1-click infection attempt. Both Viber messages and links were sent within hours of each other from the same Viber phone number and to two journalists at the same media organisation. The blurred domain and URL in Figure 2 has the same length and format as the link included in Case 1 and is most likely pointing to the same Pegasus infection domain.

Amnesty International wrote to Viber on 24 February to share information about the attack attempts sent through the Viber platform, and to highlight the potential that other Viber users were targeted by the same attacker account. In a 11 March response, a Viber representative thanked Amnesty International for reporting the issue and stated "*We undertook it for our consideration and review. Rest assured we will take measures to protect our users, if any violations are found."*

ATTRIBUTION TO SERBIAN AUTHORITIES

The NSO Group has consistently declared that "NSO products are used exclusively by government intelligence and law enforcement agencies to fight crime and terror". Indeed, in a letter to Amnesty International, NSO Group stated that that "all sales of our systems are to vetted government end-users".

Accordingly, the spyware operator is most likely affiliated with a state. In this research, Amnesty International could not identify any other governments, except for the Serbian government, as having an interest in targeting the two journalists or BIRN. BIRN and its editors and journalists have recently faced significant pressure, including online threats, physical attacks and judicial harassment through SLAPP suits. Editorial freedom and freedom of expression in Serbia have been under increasing threat, with independent outlets and reporters recently warning about a "dangerous turning point" due to mounting pressures, including "constant harassment, physical attacks and smear campaigns" orchestrated by the authorities and state-backed media. Civil society and journalists have faced an increasingly more hostile environment since the start of the student protests which have gripped the country since November 2024, after the collapse of the Novi Sad train station canopy which killed 15 people.

Amnesty International concludes that there is a strong likelihood that one or more Serbian state actors, or agents acting on their behalf, were involved in this recent use of NSO Group's Pegasus spyware to target the two investigative journalists in Serbia. It is of concern that NSO Group seems to have continued to make the Pegasus spyware available for use in Serbia despite two previous Amnesty International reports documenting the misuse of the Pegasus spyware in the country.

RESPONSIBILITY OF SERBIAN AUTHORITIES AND NSO GROUP

The discovery of two additional cases of Pegasus targeting journalists in Serbia—alongside well-documented evidence of prior abuses—points to a fundamental lack of accountability by Serbian authorities, security and intelligence services. Amnesty International wrote to the Serbian Security Information Agency (BIA, Bezbednosno-informativna Agencija) in November 2024 and again in March 2025 to seek a response to these findings but at the time of publication has not received a reply. Instead of halting the attacks and investigating their origins, the authorities in Serbia have continued with unlawful surveillance of civil society despite public exposure and criminal charges filed following Amnesty International's findings published in December 2024.

The findings also underscore that NSO Group has fallen short on preventing its products from being used to violate human rights. In December 2024, Amnesty International provided NSO Group with evidence that Pegasus was being misused in Serbia. In response, NSO Group stated it could not comment on specific past or existing customers, declining to confirm whether Serbia was a client. The company defended Serbia as "a significantly democratic and free country" and emphasized that it is "closely regulated by export control authorities," including Israel's Defense Exports Control Agency.

NSO Group also claimed to take its human rights responsibilities seriously, stating that it is "strongly committed to avoiding causing, contributing to, or being directly linked to negative human rights impacts" and that it reviews all credible allegations of misuse. However, it did not clarify whether it had investigated these findings or taken any corrective action, much less provide any evidence of doing so, as per their international human rights responsibilities.

The abuse of Pegasus in Serbia has occurred alongside reports of expanded military exports between Israel and Serbia. This inaction by NSO Group and Israeli authorities contrasts sharply with the action taken by

US-Israeli mobile forensics firm Cellebrite, which announced measures to suspend customers in Serbia following abuses documented in Amnesty International's report, "A Digital Prison".

HOW SERBIAN CIVIL SOCIETY CAN IDENTIFY POSSIBLE PEGASUS ATTACKS

Pegasus spyware can be installed through zero-click attacks, which don't require user action, and 1-click attacks, which require action from the target to enable the infection of their device, typically the opening of a malicious link.

Various social engineering techniques are used to trick the target into opening the link, including spoofing legitimate websites or news articles. If clicked on, the attack link loads an exploit chain to first compromise the web browser and ultimately install the spyware agent on the target device. The links are most often sent over messenger apps such as WhatsApp, SMS, Signal or Viber.

Amnesty International has observed multiple Pegasus infection attempts in Serbia where the Pegasus operator used a Viber or WhatsApp account registered with a Telekom Srbija phone number. In each case, the attacker messaged the target with an enticing message and a link pretending to be a news article.

Figure 3: Another Pegasus infection attempt on WhatsApp

Attackers have the option of setting a decoy website as the link destination when the attack link is disabled or when an attack attempt fails. The infection may not be triggered for a range of reasons such as the target not running a vulnerable software version, the one-time time link may already have been used, or the link may have expired.

In all Pegasus attack attempts that Amnesty International's Security Lab has observed in Serbia, the Pegasus 1-time infection links were configured to redirect to a decoy web page on a Serbia news website. This indicates the methodology used by the Serbian authorities when trying to infect targets with Pegasus, while trying to avoid suspicion or detection.

If you are a Serbian activist or civil society member, you should be cautious when receiving links from unknown Serbian phone numbers which you do not recognize. Targeted spyware attackers often adjust the message to be specific to each individual target and may include personal information about you or your

work. They may also try to create a sense of urgency to encourage you to click on a malicious link.

Reach out to the SHARE Foundation, Amnesty International's Security Lab, or trusted experts if you have received similar messages to those outlined in this blog post, and where you have reasons to believe you may have been targeted with spyware such as Pegasus due to who you are or the work you do.

Amnesty International is a movement of 10 million people which mobilizes the humanity in everyone and campaigns for change so we can all enjoy our human rights. Our vision is of a world where those in power keep their promises, respect international law and are held to account. We are independent of any government, political ideology, economic interest or religion and are funded mainly by our membership and individual donations. We believe that acting in solidarity and compassion with people everywhere can change our societies for the better.

Contact

info@amnesty.org

amnesty.org

facebook.com/
AmnestyGlobal

@Amnesty

Amnesty International
Peter Benenson House
1 Easton Street
London WC1X 0DW, UK

Index: **EUR 70/9186/2025**
Publication: **March 2025**
Original language: **English**