Exiled, then spied on: Civil society in Latvia, Lithuania, and Poland targeted with Pegasus spyware - Access Now

By Natalia Krapiva @natynettle

Archived: 2026-04-02 12:35:11 UTC

// What we found

Following last year's **joint investigation** into the use of NSO Group's Pegasus spyware against Galina Timchenko, co-founder, CEO, and publisher of *Meduza*, Access Now, **the Citizen Lab at the Munk School of Global Affairs & Public Policy at the University of Toronto ("the Citizen Lab")**, and independent digital security expert Nikolai Kvantiliani have uncovered how **at least seven more** Russian, Belarusian, Latvian, and Israeli **journalists and activists have been targeted with NSO Group's Pegasus spyware within the EU.**

// Who was targeted

One victim, who has chosen to remain anonymous, is a **member of Belarusian civil society currently based in Vilnius, Lithuania**. After receiving an **Apple threat notification** on June 22, 2023, that their device had been targeted with a state-sponsored attack, they reached out to the Citizen Lab for digital security support, who analyzed the device and **confirmed** that it was infected with Pegasus spyware on or around March 25, 2021. This date, "Freedom Day" (Dzień Voli), is a significant one, as it commemorates the Belarusian Democratic Republic's 1918 declaration of independence. Freedom Day celebrations have historically been suppressed by Belarusian officials.

Another **Russian journalist living in exile in Vilnius** since Russia's full-scale invasion of Ukraine, and who has also chosen to remain anonymous, received two Apple threat notifications on October 31, 2023, and on April 10, 2024. Access Now's Digital Security Helpline, with the **technical confirmation** of the Citizen Lab, **identified** an attempt to infect the journalist's device on or around June 15, 2023. On June 16, the journalist attended an event in Riga, Latvia, for Russian journalists in exile, which was organized by the Baltic Center for Media Excellence (BCME), DW Academy, and Sustainability Foundation. This event highlighted the ongoing vulnerabilities faced by media professionals in the region, underscoring the critical need for robust digital security measures. There were also other significant circumstances surrounding the June 15 hacking attempt that the journalist decided to keep private at this time due to personal safety concerns.

Three additional victims, all based in Riga, Latvia, **received** Apple threat notifications. Access Now's Digital Security Helpline **analyzed** their devices, with the Citizen Lab reviewing our results:

- **Evgeny Erlikh**, an Israeli-Russian journalist and the author and former producer of *Baltic Weekly*, on ***Current Time***, RFE RL's 24/7 Russian-language TV network. Our analysis showed that Erlikh's iPhone was infected with Pegasus spyware between November 28 and 29, 2022. At the time, Erlikh was

vacationing in Austria with his spouse, who also received an Apple threat notification, but we were unable to forensically analyze her phone.

- **Evgeny Pavlov**, a Latvian journalist, former correspondent for ***Novaya Gazeta Baltija***, an independent news media covering the Baltic countries, and former freelance journalist for *Current Time's Baltia* program. Pavlov's device was targeted with Pegasus on or around November 28, 2022, and on or around April 24, 2023; however, we were unable to confirm if the attempts were successful.
- **Maria Epifanova**, general director of ***Novaya Gazeta Europe*** and director of *Novaya Gazeta Baltija.* Epifanova's iPhone was infected on or around August 18, 2020 — the earliest known use of Pegasus to target Russian civil society. Epifanova was chief editor of *Novaya Gazeta Baltija* at the time, and the attack occurred shortly after she received accreditation to attend exiled Belarusian democratic opposition leader Svetlana Tikhanovskaya's **first press conference in Vilnius**.

Two Belarusian civil society members currently living in Warsaw, Poland, also received Apple notifications on October 31, 2023:

- **Andrei Sannikov** is a prominent Belarusian opposition politician and activist, who ran for President of Belarus in 2010, receiving the **second highest vote** count after incumbent Alexander Lukashenko. After the election he was **arrested by the Belarusian KGB** and held as a prisoner of conscience. Authorities also threatened to **take away his three-year old son**. **According to the Citizen Lab**, Sannikov's iPhone was infected with Pegasus on or around September 7, 2021.
- **Natallia Radzina** is editor-in-chief of independent Belarusian media website **Charter97.org** and a **recipient** of the Committee to Protect Journalists (CPJ) International Press Freedom Award. Radzina was persecuted for journalistic activities in Belarus, imprisoned, and forced to flee the country. **Access Now's Digital Security Helpline**, as **confirmed** by the Citizen Lab, also identified that Radzina's device was infected with Pegasus spyware on or around December 2, 2022, December 7, 2022, and January 16, 2023. The first infection took place the day after Radzina's participation in the **Third Anti-War Conference** in Vilnius, organized by the Free Russia Forum.

// New patterns emerge

Our investigation shows that the use of Pegasus spyware to target Russian- and Belarusian-speaking journalists and activists dates back until at least 2020, with more attacks following Russia's full-scale invasion of Ukraine in February 2022.

Access Now and the Citizen Lab also confirmed that five of the victims' phones contained Apple IDs used by Pegasus operators in their attempts to hack the devices. We know that targeting via **various exploits** that take advantage of bugs in *HomeKit* can leave a record of the attacker's Apple ID email address on the victim's device. The Citizen Lab believes that each Apple ID is used by a single Pegasus operator, though a single Pegasus operator might use multiple Apple IDs. We **found** the same Apple ID email address present on Pavlov, Radzina, and the second anonymous victim's phones. A separate email account was used to target both Erlikh and Pavlov's phones on November 28, 2022. Artifacts from Andrei Sannikov and Natallia Radzina's phones contained another separate identical email, **according to the Citizen Lab**. This suggests that a single Pegasus spyware operator may be behind the targeting of at least three of the victims and possibly all five.

// Who is responsible?

Access Now and the Citizen Lab are not publicly naming a specific operator at this time. Given that Poland has not been documented as targeting victims outside the country with Pegasus spyware, and considering **reports** that Poland's government stopped using Pegasus spyware in 2021, it is unlikely that Poland is behind the attacks mentioned in this investigation. The Citizen Lab tells us that there is also no evidence suggesting that Russia, Belarus, or Lithuania are Pegasus customers. Latvia **appears to use Pegasus**, but the country is also not known for targeting victims outside of its borders. Estonia is another Baltic state that **cooperates closely with Latvia and Lithuania on security matters**, including regarding **Russia and Belarus**. According to the Citizen Lab, Estonia does appear to use Pegasus extensively outside their borders, including within multiple European countries.

// The investigation continues

Access Now, the Citizen Lab, and other partners continue investigating these attacks against journalists, activists, and dissidents in exile and at home. We advise members of civil society to follow **digital security recommendations**, which include updating your devices' software or implementing **Apple Lockdown Mode**. If you received an Apple threat notification or suspect your device may have been targeted with spyware, contact **Access Now's Digital Security Helpline**; support is available in nine languages including **Russian**.

In the meantime, Access Now **urges** all governments to establish an immediate moratorium on the export, sale, transfer, servicing, and use of targeted digital surveillance technologies until rigorous human rights safeguards are put in place to regulate such practices, and to ban the use of spyware technologies such as Pegasus that have a history of enabling human rights abuses.
