Hacking Meduza: Pegasus spyware used to target Putin's critic

By Natalia Krapiva @natynettle

Archived: 2026-04-06 00:13:31 UTC

An investigation by Access Now and the Citizen Lab at the Munk School of Global Affairs at the University of Toronto (the Citizen Lab) has revealed that the iPhone of journalist Galina Timchenko, head of *Meduza*, a leading Russian independent media outlet based in Latvia, has been infected with Israeli firm NSO Group's Pegasus spyware. The spyware attack took place two weeks after the Russian government declared *Meduza* an "undesirable organization" for its critical coverage of Vladimir Putin's regime and the war in Ukraine. At the same time, some European political leaders were publicly arguing for surveillance of all Russians in exile. This is the first documented case of a Pegasus infection of a Russian journalist.

// What happened

On June 22, 2023, Timchenko, co-founder, CEO, and publisher of *Meduza*, received a notification from Apple that state-sponsored attackers may be targeting her iPhone. The next day, *Meduza*'s Chief Technology Officer contacted Access Now to check the phone for traces of spyware. Access Now, with forensic assistance from the Citizen Lab, tested the device, and discovered that it had been infected with Pegasus spyware on or around February 10, 2023, with the infection likely lasting several days or weeks after that. At the time of the infection, Timchenko, who lives in Latvia, was in Berlin, attending a private gathering organized by Redkollegia with other members of Russian independent media living in exile to discuss the legal risks of "undesirable" and "foreign agent" designations.

The Pegasus attack was conducted within the larger context of attacks against *Meduza* and other Russian independent media organizations, at home and in exile.

Timchenko and her colleagues founded *Meduza* in 2014, after the owner of *Lenta.ru* removed her as the chief editor for publishing an interview with the head of a Ukrainian nationalist group. The organization chose to base *Meduza* in Latvia, relying on digital technologies to reach audiences inside Russia. The publication became one of the first independent media outlets run by Russian journalists in exile to launch a mobile app as a means of circumventing Russian censorship.

Meduza's critical coverage did not, however, go unnoticed by Putin's regime. In 2019, Russian police arrested *Meduza* journalist Ivan Golunov on fabricated drug charges. After public outcry, Golunov was subsequently released, and the police officers involved were sent to prison for the unlawful arrest. In 2021, the Russian

government designated *Meduza* a "foreign agent," a move condemned by the E.U. and media freedom organizations, among others. In March 2022, due to *Meduza*'s critical coverage of Russia's full-scale invasion of Ukraine and condemnation of the war, the government went even further and blocked *Meduza*'s website. Finally, in January 2023, Putin's regime officially outlawed *Meduza*, classifying it an "undesirable organization," a more serious designation. This action drew strong condemnation from the Organization for Security and Cooperation in Europe (OSCE), International Press Institute, European Federation of Journalists, and others.

Other independent media organizations, such as *TV Rain*, *The Insider*, *Novaya Gazeta*, *The Moscow Times*, *Mediazona*, *DOXA*, as well as human rights NGOs, like Memorial, OVD-Info, Golos, Sakharov Center, and many others, have likewise faced escalating persecution in recent years, especially since Russia's 2022 full scale invasion of Ukraine. They have been targeted under various designations, blocked, banned, and disbanded.

In addition, *Meduza*, like many other Russian independent media and human rights organizations, was also heavily impacted by tech and financial companies' over-compliance with sanctions against Russia. Blocked and criminalized in its own country, *Meduza* was unable to receive donations from supporters inside Russia due to Western payment services pulling out. Despite the enormous financial challenges, the organization continued to do its work.

Horrifically, Russian independent journalists have also faced suspected poisoning attacks while seeking refuge in Europe. In October 2022, Elena Kostyuchenko, *Novaya Gazeta* and *Meduza* journalist, was allegedly poisoned in Germany. Her symptoms were similar to those experienced by other Russian journalists, activists, and dissidents criticizing Putin's regime.

// Who is behind this Pegasus attack?

Pegasus is designed to obfuscate which government is behind a particular attack, making it difficult for us to attribute. However, based on NSO Group's assertion that Pegasus is only sold to state agencies and the available technical and circumstantial evidence, there are several theories of which state is likely behind the attack.

Meduza's host state, Latvia, could have been responsible, as they appear to be a Pegasus customer. However, according to the Citizen Lab, there has not been any indication of Latvia using Pegasus to spy outside of its borders. Germany, where Timchenko was staying at the time of her phone's infection, is another potential culprit, as they also appear to be a Pegasus customer, although the reported German customer is a police agency, rather than an intelligence agency. Two other reported European Pegasus customers, the Netherlands' General Intelligence and Security Service (AIVD) and an unnamed Estonian government agency, appear to use Pegasus extensively outside their borders, including within multiple European countries, according to the Citizen Lab. While there are claims that NSO Group does not allow Estonia to target Russian phone numbers, Timchenko's phone number has a Latvian country code (+371).

The E.U. PEGA Committee revealed at least 14 E.U. states and 22 operators of Pegasus in the E.U. In fact, just two months before Timchenko's phone was infected, Latvia declared another independent media organization in exile — TV Rain — to be "a threat to the national security and public order" and canceled its license. This decision was criticized by the Latvian Association of Journalists as "disproportionate." Other E.U. leaders, like the president of the Czech Republic, Petr Pavel, have publicly stated that all Russians living in the West should be put

under “strict surveillance” as the price of Russia’s war against Ukraine. The public pressure on E.U. leaders to demonstrate support for Ukraine in the face of Russia’s aggression may be deepening the risks for Russian independent media groups like *Meduza* that are already in danger because they seek to hold Putin accountable.

Another possibility is that states with ties to Russia that are suspected Pegasus users — Azerbaijan, Kazakhstan, or Uzbekistan — may have hacked *Meduza* on behalf of Russia. In May 2023, an investigation by Access Now and partners revealed that Azerbaijan is a potential culprit behind the targeting of media workers and other civil society actors in Armenia. Notably, Kazakhstan itself has blocked *Meduza* over a controversial article. However, according to the Citizen Lab, there is no evidence of Azerbaijan or Kazakhstan targeting people in Germany, Latvia, or other E.U. states. Also, Uzbekistan is not believed to have been a Pegasus customer during the period in question.

Finally, as we have seen with the state targeting of independent media and journalists in countries from El Salvador to Hungary, it is possible Timchenko’s own government — Russia — is behind the hacking. As we have noted, the attack happened just two weeks after Russia designated *Meduza* an “undesirable organization,” which, unlike the “foreign agent” designation, immediately criminalizes all activities of an organization, requiring it to shut down. *Meduza* also experienced a spike in digital attacks in February 2023; for example, attackers blocked mirror websites, and engaged in phishing and other efforts to compromise user accounts. However, according to the Citizen Lab, there is currently no evidence that the Russian government is operating the Pegasus system. Experts on Russia’s intelligence services, like journalist Andrei Soldatov, are not convinced that Russia has been using Pegasus.

// Spyware violates human rights and international humanitarian law

Whether during war or peace, surveillance of journalists and independent media by intrusive spyware like Pegasus is prohibited under E.U law, international human rights law, and international humanitarian law.

Sophisticated spyware like Pegasus, which bypasses encryption and takes full control of the victim’s phone, including access to photos, messages, and contacts, as well as the phone’s camera and microphone, represents an existential threat to journalists and media freedom globally. Such spyware jeopardizes journalists’ ability to safely do their work and protect the confidentiality of their sources. Civil society has documented that it can also facilitate domestic and transnational repression and serious human rights violations, including torture, enforced disappearance, and extrajudicial killings, such as the murder of the *Washington Post* journalist Jamal Khashoggi.

UN officials, the European Parliament, the European Data Protection Supervisor, and civil society actors from around the world have widely condemned the use of spyware against journalists and human rights defenders. The U.S. government has placed NSO Group and other spyware makers on its Entity List and has banned the federal government from using certain commercial spyware due to the severe human rights and national security risks. The International Committee for Red Cross and Red Crescent (ICRC) experts have stated that the use of spyware against civilians in a context of conflict “exposes civilians to harm, affects their rights, safety, and dignity.”

// Call for action

All States

➡️ Implement 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;

➡️ Where there is evidence that commercial spyware technology facilitates or enables human rights abuses, implement a ban on said technology and its vendors;

➡️ Hold the companies who develop and distribute these technologies, and their investors, accountable for their failure to respect human rights and for the role they play in enabling abusive end uses, and demand transparency from said companies around their clients and practices, in particular regarding their data collection and processing practices;

➡️ Reaffirm protections for all journalists and media workers and safeguard press freedom, by recognizing that journalists and media workers are not legitimate surveillance targets for practicing their work;

➡️ Ensure prompt, impartial, and independent investigation into the hacking allegations and establish accountability and remedy mechanisms for surveillance victims;

➡️ Fully cooperate with European Court of Human Rights, the UN, and all regional and international investigative bodies and accountability mechanisms with respect to investigation of Pegasus hacking and other unlawful surveillance;

➡️

Impose sanctions on NSO, its staff, and all of their technologies as a threat to human rights, media freedom, peace, and security.

Russia (in addition to the recommendations for all other states)

➡️ End its illegal aggression against Ukraine and attacks on independent media, civil society, and regime critics in Russia and in exile;

➡️ Comply with international human rights obligations, including in relation to the rights of freedom of expression, peaceful assembly, and association. This includes ending all digital and physical repression including censorship, surveillance, designation of organizations as foreign agents, undesirable, terrorist/extremist, criminalization of protected speech, and targeting and incarceration of political prisoners, as well as revoking the laws that enable this repression.

If you are a journalist, activist, human rights defender, or another member of civil society, and you suspect you may be a victim of spyware, please contact Access Now's Digital Security Helpline at help@accessnow.org (we speak Russian and Ukrainian, among other languages).

If you want to support *Meduza*, join their crowdfunding campaign.

Source: https://www.accessnow.org/publication/hacking-meduza-pegasus-spyware-used-to-target-putins-critic/