Pegasus spyware infections of civil society victims in Latvia, Lithuania, and Poland in 2022 and 2023: a technical brief

This technical brief outlines efforts by Access Now's Digital Security Helpline ("the Helpline") to obtain and analyze forensic evidence of attacks deploying NSO Group's Pegasus spyware against members of civil society living in Latvia, Lithuania, and Poland.

This document covers only a subset of the identified victims. In these cases, the Helpline found that the Pegasus spyware attacks, which exploited HomeKit vulnerabilities, were deployed using the same operator iCloud accounts. It seems unlikely that iCloud accounts are shared between different Pegasus operators. This suggests a common Pegasus operator, although we are not presently attributing the operator.

Additional cases are described in the broader report ***"Exiled, then spied on: Civil society in Latvia, Lithuania, and Poland targeted with Pegasus spyware"***, by Access Now in collaboration with the Citizen Lab at the Munk School of Global Affairs & Public Policy at the University of Toronto ("the Citizen Lab").

I. Background

Access Now's Digital Security Helpline provides real-time, direct technical assistance and advice to civil society groups, activists, media organizations, journalists, bloggers, and human rights defenders worldwide. Its Analysis and Forensics team conducts root-cause analysis in security incidents, including in the potential use of surveillance technologies to restrict the rights of at-risk communities.

To ensure the quality and safety of its services, the Helpline carefully vets potential beneficiaries by conducting research and basic human rights due diligence, with the support of its network of trusted partners. The activities leading to the following brief involved the confirmation that all victims aided in this report are indeed members of civil society who have made positive contributions to their communities.

After establishing contact with the victims, the Helpline conducted a process aimed at assisting them to detect, diagnose, and overcome abuses against their right to privacy and other human rights. The work of the Helpline seeks to support and empower them in overcoming these challenges, by providing technical support and guidance. The analysis methodology used in this investigation has been independently reviewed and confirmed by the Citizen Lab.

II. Findings

Between 2022 and 2023 the Access Now Digital Security Helpline analyzed logs from iPhone devices belonging to Russian, Belarusian, Latvian, and Russian-Israeli journalists who live in Europe. Our analyses concluded that several of these devices were targeted and/or successfully compromised with NSO Group's Pegasus spyware.

Several of the phones showed evidence that they had been targeted by an exploit for HomeKit, such as PWNYOURHOME. The attacks against three of the victims were conducted with the same Apple ID, with an additional, separate Apple ID also overlapping between two victims. This overlap, along with other circumstances surrounding the attacks, indicates that at least three, and possibly all four, were likely targeted by the same operator.

The table below summarizes the dates of these attacks based on the device logs analyzed for this report. If the logs show that some stage of the Pegasus spyware ran on the device, the attack is marked as an *Infection*. If the logs do not conclusively show that the Pegasus spyware ran on the device, but there are traces of an attack, then we mark the attack as an *Attempt*.

Victim code / name / SN	Affiliation	Date of infection / attempt	Attacks
Evgenry Erlikh	Journalist	Between 2022-11-28 and 2022-11-29	Infection using HomeKit exploit
Evgenry Pavlov	Journalist	2022-11-28	Separate attempts to use a HomeKit exploit

		2023-04-24	
Anonymous	Journalist	2023-06-15	Attempt to use a HomeKit exploit
Natallia Radzina	Journalist	On or around 2022-12-02 On or around 2022-12-07 On or around 2023-01-16	Infection using HomeKit exploit

III. Acknowledgments

The Digital Security Helpline extends its gratitude to members of civil society who were targeted in these attacks for their trust and their crucial role in this investigation. Their collaboration and commitment to the pursuit of truth was vital in this project.

We acknowledge the Citizen Lab team for their valuable support and mentoring, which greatly contributed to the progress of this investigation.

We would like to acknowledge the contributions of the Amnesty Tech team for sharing their Mobile Verification Toolkit, an important asset during this project.

VI. Contacts

If you have any questions or require further information regarding this report and the ongoing investigation, please reach out to Access Now at press@accessnow.org. We welcome your inquiries and are here to provide any clarifications you may need.