The inside view of spyware's 'dirty interference,' from two recent Pegasus victims

By Suzanne Smalley

Published: 2024-06-25 · Archived: 2026-04-06 01:08:08 UTC

Andrei Sannikov challenged longtime Belarusian dictator Aleksandr Lukashenko in the country's 2010 national elections, a move that landed him in jail for 16 months, provoked threats that his young son would be taken by the state and led him to flee the country after his release from prison due to death threats.

Sannikov has spent every day since his escape trying to undermine Lukashenko, leading a campaign promoting the integration of Belarus into the European Union by writing books, speaking at universities and attending conferences with other freedom fighters.

"My goal is to go back to a free Belarus," said Sannikov, who now lives in exile in Poland.

Perhaps it's no surprise, then, that Sannikov is one of seven Russian- and Belarusian-speaking activists and journalists living in exile whose phones were recently discovered to have been targeted by or fully infected with powerful commercial spyware known as Pegasus, according to a recent report published by the digital civil rights group Access Now.

Five of the seven victims' devices were infected with Pegasus, while two others had an attempted breach or, in one case, could not be confirmed with an infection.

The findings about Sannikov and the six other victims are part of a broader ongoing probe into Pegasus attacks against similar people in the region, Recorded Future News has learned. The powerful spyware has become a threat to activists, political opposition figures and journalists around the globe as authoritarian and even many democratic governments deploy it outside its intended use for fighting crime and terrorism.

Sannikov worries about Pegasus, he said in an interview, because "there are no effective means to prevent it and to fight it."

"If the software spreads then we will be vulnerable in every part of the world," he added.

Another of the seven victims to speak with Recorded Future News, Evgeny Erlikh, works in Latvia on a U.S.-funded Radio Free Europe/Radio Liberty news program designed for a Russian-speaking audience. He believes he is likely one of several additional and so far mostly unknown Latvia-based journalists to be hit with Pegasus.

Digital forensic researchers are now studying the devices of other potential victims with similar profiles, according to Natalia Krapiva, senior tech legal counsel at Access Now.

Even as Pegasus is showing up on an increasing number of phones belonging to civil-society organizations and individuals, experts and victims say they are bracing for usage of the powerfully invasive spyware to grow

exponentially.

The newly discovered infections are just the “tip of the iceberg,” Sannikov said, echoing Ehrlikh’s contention that many victims in his community likely remain unknown.

The tip of the iceberg

Six of the seven new victims received Apple threat notifications, which are warnings that say an iPhone may have been targeted by mercenary spyware. The alerts are sent to users by email and iMessage as well as in a red-lettered display after they sign into their device with their Apple ID.

Sannikov did not receive a threat notification from Apple and instead learned of the infection when he turned over his phone for a free security check offered at a large conference he attended in November 2023.

“It was quite a coincidence that I submitted my phone,” Sannikov said.

The random nature of the discovery of Pegasus on his phone suggests to him that a much larger number of Belarusian and Russian opposition leaders and journalists could unknowingly own infected devices, he said. Still others may have been breached but chosen not to go public.

“There might be hundreds or even thousands of cases because I spoke to the people, especially those who are in the opposition and Russian and Belarusian journalists, and they said that they were hacked and they were infected,” he said.

Digital forensic researchers found Sannikov’s phone was compromised in September 2021 at a time when the opposition leader said he was attending a prominent conference in Poland. A large number of opposition politicians, journalists, civil society activists and major public figures were among the 5,000-plus attendees.

> "For me, it was clearly a very dirty interference in my private life."
>
> *— Andrei Sannikov*

A seasoned activist, Sannikov said he doesn’t trust any electronics and never discusses sensitive work-related information on his phone or computer.

His personal communications are a different story.

“It was creepy,” he said in an interview. “There were a lot of personal conversations which are not meant for anybody's ears. … For me, it was clearly a very dirty interference in my private life.”

A spokesperson for the NSO Group said that it cannot confirm or deny specific customers for regulatory reasons, but did reiterate that it does not sell Pegasus to Russia or its allies.

“NSO complies with all laws and regulations and sells only to vetted intelligence and law enforcement agencies,” the spokesperson said via email. “Our customers use these technologies daily to prevent crime and terror attacks.”

A chilling effect

Sannikov doesn't think it is random that his phone was breached when he was at a conference mingling with politicians, journalists and other public figures.

The larger pattern supports his thesis: Four of the seven newly revealed victims were attacked or infected immediately before, while or after attending similar conferences, meetings or, in one case, a press conference with a Belarusian opposition leader.

Last February, an iPhone belonging to Galina Timchenko, a prominent Kremlin critic, also was compromised on the eve of a gathering with like-minded journalists, according to digital forensics researchers. Timchenko, the owner of the independent Latvia-based news organization Meduza, was infected the day before she attended a private meeting in Berlin with other exiled Russian-speaking reporters, the researchers said.

"Pegasus creates a chilling effect on human rights by making journalists and activists scared to talk to their sources and attend human rights conferences out of fear they are being surveilled," said Krapiva of Access Now.

The software allows astonishing access to devices. It is typically zero-click — meaning that a recipient's device only needs to receive the file for it to be activated — and once installed can activate a phone's microphone and camera, allowing Pegasus operators to not only access emails, text messages, live phone conversations and call histories belonging to a given phone's owner, but also spy on bystanders who are speaking with a victim whose phone is nearby.

It is impossible to know with certainty that a device is infected with advanced commercial spyware without having it checked by experts. Sometimes even they can't detect infections. With advanced commercial spyware, experts say, we don't know what we don't know.

While it is unclear who is responsible for any of the seven new attacks, five of the seven devices analyzed in the new report "recorded Apple IDs used by Pegasus operators in their hacking attempts," according to researchers from The Citizen Lab, a University of Toronto-based digital security and human rights research group, which worked with Access Now investigating the digital forensics of the attacks.

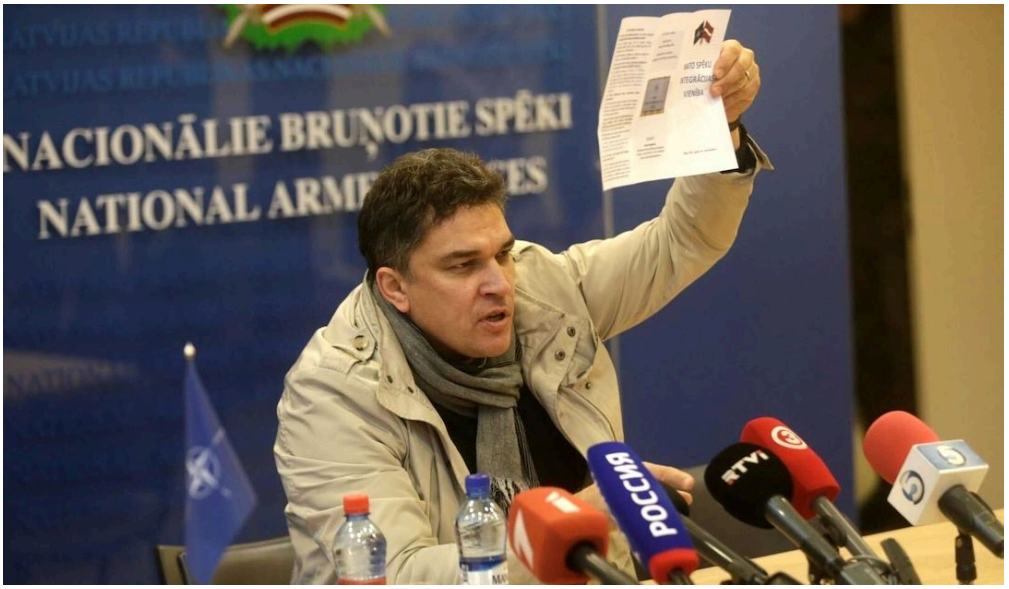
"The targeting timeframe, victim profiles, and overlap of operator Apple IDs suggest (but do not prove) the possibility that a single actor is responsible for these five attacks," a Citizen Lab blog post said.

A Latvian connection?

There is no evidence that Russia or Belarus are Pegasus customers, and Poland stopped using the spyware in 2021, Access Now says.

Latvia appears to use the spyware but is not known for deploying it against people in other countries, according to the researchers, who also said that neighboring Baltic nation Estonia coordinates with Latvia and Lithuania on security matters and does use Pegasus extensively across Europe.

Erlikh, the journalist who produces a Radio Free Europe/Radio Liberty news show, worked for years in Russia, including as a correspondent in Chechnya. His phone was found to be infected with Pegasus in 2023.



Evgeny Erlikh at a press conference in Latvia in 2015. Image courtesy of Evgeny Erlikh

He thinks it is notable that he, Timchenko and a third victim named in the new report, Maria Epifanova, were among the first Russian journalists to move to Latvia and establish offices in Riga, all around 2014 when Russia annexed Crimea and invaded Ukraine for the first time.

Around then, Erlikh says, Baltic countries like Latvia started worrying they might be the next victims of Russian aggression.

An iPhone belonging to Epifanova, general director of Novaya Gazeta Europe, a Russian language outlet, was infected on or around August 18, 2020, which is the "earliest known use" of Pegasus to target Russian civil society, according to Access Now. The infection coincided with Epifanova seeking accreditation to attend a press conference hosted by a prominent Belarusian opposition leader.

"Maybe Latvian intelligence had to check the validity of foreign Russian opposition journalists to ensure they were not Russian spies," Erlikh told Recorded Future News.

"Perhaps someone wanted to use us to infiltrate the local community of Russian-speaking, emigrant, opposition journalists to understand who they are, what they say, and whether there are any dubious characters among them," he added.

Erlikh said his Pegasus infection hasn't made him feel less safe in Latvia, but has "made us realize that apparently they [Latvian state officials] are noticing us."

He called the recently surfaced cases "just a drop in the ocean."

"If those behind the infection really wanted to know how Russian opposition journalists live in exile, then there are many, many more such infections," Erlikh said. "Right now, we're talking about the visible part."

A spokesperson for the Latvian Embassy in Washington said via email that spyware is an international problem and emphasized that Pegasus can be installed from any location despite the fact that the impacted journalists are based in Latvia.

“In Latvia, wiretapping and other operational activities are regulated by the Operational Activities Law,” the spokesperson said. “Wiretapping is carried out only with a permission issued by the judges of the Supreme Court of Latvia.”

“Security agencies do not publicly comment on the methods used in their operations,” the spokesperson added.

A dangerous technology spreads

The NSO Group says it only sells Pegasus to vetted law enforcement and intelligence agencies that agree to use the technology to investigate legitimate targets, but the company won’t divulge any further information — including which national governments are customers. However, in recent years Pegasus has been found on devices belonging to members of civil society or political opposition leaders in Spain, Greece, Hungary, Poland, India, El Salvador, Thailand and Latvia, among many other countries.

In February, a random security check of iPhones belonging to European Parliament members and staff turned up traces of spyware on devices belonging to two members and an adviser working on the body’s Subcommittee on Security and Defense, highlighting the likelihood that some people who do not undergo random checks may unknowingly be victims of attempted hacks or infections.

Polish officials announced in April that nearly 600 people, some of whom were opposition politicians and their supporters, were targeted with Pegasus between 2017 and 2022. The mass surveillance effort is now being probed by Poland’s national prosecutor.

“These cases raise troubling questions, especially against the backdrop of Europe's puzzlingly poor track record on mercenary spyware accountability and transparency,” said John Scott-Railton, a senior researcher at The Citizen Lab.

In a June 14 court filing, NSO Group said it believes members of political opposition are legitimate Pegasus targets because they are “senior political operatives” and can be probed for “legitimate intelligence investigations.”

Calling himself “the last person who should be hacked,” Erlikh, like Sannikov, focused on the intrusion into his personal life.

“Maybe they learned what color my underwear is,” he said. “Maybe such intimate details are now known to them.”

Vowing not to be silenced, Erlikh said he won’t stop doing work that draws the attention of those in power.

“They could not intimidate us,” he said. “We are not scared.”

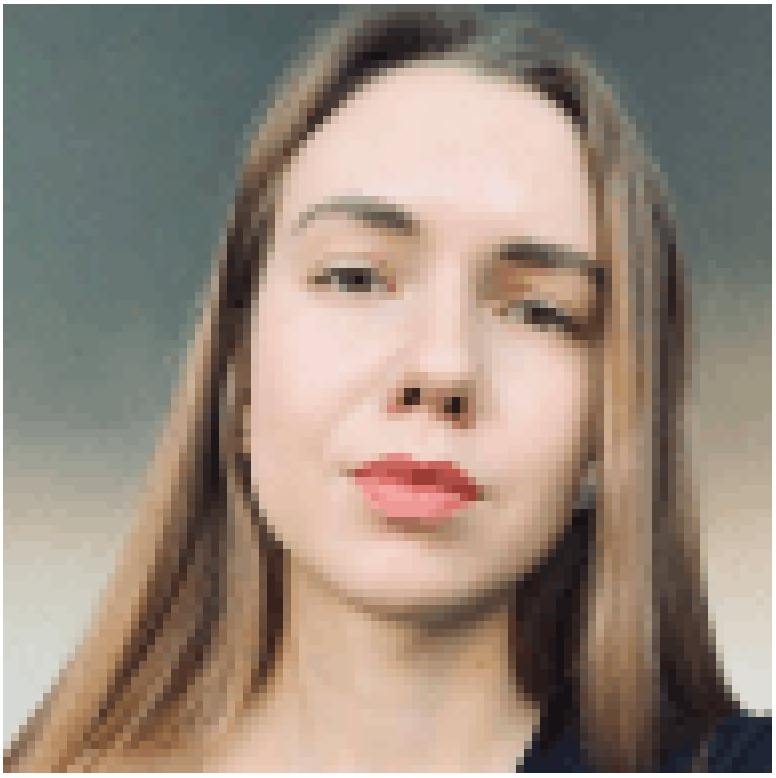
Editor's Note: Story updated June 26 with a statement from the Latvian Embassy in Washington.

No previous article

No new articles

Suzanne Smalley

is a reporter covering digital privacy, surveillance technologies and cybersecurity policy for The Record. She was previously a cybersecurity reporter at CyberScoop. Earlier in her career Suzanne covered the Boston Police Department for the Boston Globe and two presidential campaign cycles for Newsweek. She lives in Washington with her husband and three children.



Daryna Antoniuk

is a reporter for Recorded Future News based in Ukraine. She writes about cybersecurity startups, cyberattacks in Eastern Europe and the state of the cyberwar between Ukraine and Russia. She previously was a tech reporter for Forbes Ukraine. Her work has also been published at Sifted, The Kyiv Independent and The Kyiv Post.
