Exiled Russian journalist hacked using NSO Group spyware

Publication Date: 2023-09-13

Author: Stephanie Kirchgaessner

Section: Technology

Tags: Hacking, Espionage, Press freedom, Russia, Europe, news

Article URL: https://www.theguardian.com/technology/2023/sep/13/exiled-russian-journalist-galina-timchenko-reportedly-hacked-using-nso-group-spyware

An award-winning Russian journalist living in exile in Europe was hacked using Israeli spyware made by NSO Group, according to a joint investigation by the Citizen Lab and Access Now. Galina Timchenko was hacked on or around 10 February, at a time when she was based in Berlin, Germany, marking the first time that an independent Russian journalist – whose media outlet has been targeted by Moscow and declared an "undesirable organisation" – is known to have been hacked with spyware. The attack occurred shortly before a meeting in Berlin of the main independent Russian media in exile, in which participants including Timchenko discussed the pressure they were under and how to respond to it. It was organised by a Russian organisation called Redkollegiya. "Through me they could have eavesdropped on this meeting," the journalist said in an interview with the Guardian. Once a phone is infected with Pegasus – NSO's signature spyware – the operator of the hacking software has total control over a phone, including access to photos, encrypted apps and the microphone, which allows the user to turn the mobile into a listening device. The news has raised questions about who might have been behind the attack. Researchers said they were not immediately able to identify who might have targeted Timchenko's phone, but said it was hacked using Pegasus, one of the world's most sophisticated military-grade spyware tools. Russia would be considered an obvious candidate to have targeted Timchenko, who is the co-founder and chief executive of Meduza, an independent Russian news website that has a record of publishing critical articles about the war in Ukraine and investigations into the Russian elite, including those close to Vladimir Putin. NSO, which is closely regulated by the Israeli government, sells only to government agencies. The company is known to sell to authorities in many European countries – including the German police – and countries in the Middle East and Africa. Timchenko told the Guardian she personally believed that Russia was ultimately behind the hacking of her phone. "Before this, all the other attacks were from Russia. We've had a number of different attacks and they were all from Russia. So if it swims like a duck, quacks like a duck, it's probably a duck," she said. But the Citizen Lab and Access Now, two of the world's experts on surveillance and spyware, said they believed it was "unlikely" that Russia was a client of NSO Group, and emphasised that they had not seen any other indications from research that Moscow might be behind the attack. The declaration left a few other possible options, the researchers said. Meduza is based in Latvia, which appears to be an NSO Group customer. But researchers said there was no evidence that Latvia had the ability to use Pegasus software outside its own border. Germany is a known client, too, but the researchers said they believed it was unlikely that a German police agency – which is believed to use Pegasus – had targeted Timchenko. The Netherlands intelligence and security service, the Dutch intelligence agency, and an

Estonian government agency both appear to use Pegasus outside their jurisdiction, including within Europe. The Guardian has previously reported that Estonia, a Nato member, acquired access to Pegasus in 2019 but was informed by NSO in August that year that the company would not permit Estonian officials to use the spyware against Russian targets. Timchenko was using a Latvian country code at the time she was hacked. “It is plausible that one of these agencies was targeting Timchenko although it would be unclear under what justification,” researchers said. They added that it was possible that a Russian ally known to be a Pegasus customer could be behind the spying on behalf of Russia, including Azerbaijan or Kazakhstan, though researchers said they had never observed attacks against individuals living in the EU by either country. NSO does not disclose the names of its clients. But a spokesperson appeared to suggest that Russia was not a client. In a statement, the spokesperson said: “NSO only sells its technologies to allies of the US and Israel and always investigates credible allegations of misuse, taking prompt action if warranted.” The company has said it sells its spyware to countries to be used only to fight serious crime and terrorism threats. It has also denied having any knowledge or control of individuals who are targeted once their spyware licences are sold to government clients, who then operate the hacking software. Timchenko said the attack against her was disconcerting, because she had never considered herself of interest to the security services. “I haven’t engaged in journalistic work for some time. I’m not part of the editorial board. I don’t know what they are planning. I deal with publishing, new projects, money, contracts,” she said, adding that it was a similar sensation to having one’s wallet stolen. “There’s nothing really there but those are your things, it’s very uncomfortable,” she said. However, she acknowledged she was concerned about the exposure of her contact list. Meduza was declared an “undesirable organisation” by the Russian government earlier this year, making it virtually impossible to conduct reporting or collect revenue in the country. Before founding Meduza, Timchenko was the editor of Lenta.ru, an extremely popular website that pioneered online news in Russia. Timchenko was fired by Lenta.ru’s billionaire owner due to her team’s reporting on the 2014 Ukraine crisis. The decision sparked a staff revolt that resulted in Timchenko co-founding Meduza in Riga, Latvia, where she believed the website would have more protection from the Russian government and Kremlin-friendly business people. She is one of the most prominent Russian journalists outside the country. She appears regularly at academic forums and events, including those that attract prominent figures in the Russian opposition and émigré communities. The attack was condemned by Sophie in ‘t Veld, a Dutch MEP and high representative for foreign affairs and security policy. In a tweet she said: “3 years of revelations, parliamentary&judicial inquiries, US blacklisting and public outcry, but the abuse of #spyware #Pegasus continues right under our noses.” The investigation began after Apple warned Timchenko and other targets in June 2023 that they may have been targeted with spyware.