GlobalResearch
Center for Research on Globalization

First Documented Case of Pegasus Spyware Used in an International War Context. Report

The report concludes that “the targeting is related to the military conflict in Nagorno-Karabakh.”

By Arzu Geybullayeva
Global Research, May 30, 2023
Global Voices 25 May 2023

Region: Europe
Theme: Intelligence

***

A new investigation reveals the use of Pegasus spyware in an international war context.

The report, released on May 25, is a joint investigation between Access Now, CyberHUB-AM, the Citizen Lab at the Munk School of Global Affairs at the University of Toronto (the Citizen Lab), Amnesty International’s Security Lab, and an independent mobile security researcher Ruben Muradyan.

According to its findings, at least 12 Armenian citizens were targeted with the spyware between October 2020 and December 2022. The list includes Armenia’s Ombudsperson, two Radio Free Europe/Radio Liberty (RFE/RL) Armenian service journalists, a United Nations official, a former spokesperson of Armenia’s Foreign Ministry, and seven other representatives of Armenian civil society.

The evidence collected and presented in the report demonstrates that “the targeting is related to the military conflict in Nagorno-Karabakh.”

> BREAKING: We reveal how NSO Group’s Pegasus spyware is being used in the Azerbaijan-Armenia war — first time recorded in international armed conflict.
>
> There are at least 12 civil society targets incl. journalists, human rights defenders + activists.https://t.co/U6d9PokUvN
>
> — Access Now (@accessnow) May 25, 2023

Forensic investigation of devices indicated the following exploits used in Armenia:

PWNYOURHOME, FINDMYPWN, FORCEDENTRY (also referred to as Megalodon by Amnesty's Security Lab), and KISMET. All these exploits were revealed and under investigation by Citizen Lab since 2020, but it were Armenian cases that helped Citizen Lab to first identify PWNYOURHOME exploit which was at the center of the most recent investigation published in April 2023.

According to the joint recent investigation published on May 25, the timing of infections was an indication of its relevance to the conflict between Armenia and Azerbaijan, and was likely "the reason for the targeting":

> The backdrop of the first cluster of civil society Pegasus infections found in Armenia is the bloody 2020 Nagorno-Karabakh war with Azerbaijan, the associated peace talks in October 2020, and the November 9, 2020 ceasefire agreement. At the same time, the Karabakh conflict itself began to intensify again with the Azerbaijan May 12, 2021 offensive and more clashes in July and November 2021. The majority of the Armenia spyware victims were infected during this time period in 2020-2021; between them, there were over 30 successful Pegasus infections.

In total, the forensic investigations identified over 40 infections and one failed attempt.

The report then dives into the identified cases, presenting the findings of the investigation. Five of the identified targets preferred to stay anonymous at the time of the report's release.

The culprits

The authors of the report note that they have not been able to "conclusively link this Pegasus hacking to a specific governmental operator." According to investigations published to date, Armenia was not among the list of clients identified as having purchased NSO's Spyware. Azerbaijan, on the other hand, was. The use of Pegasus and other spyware technology used against civil society in Azerbaijan has been widely documented in recent years.

According to the Organized Crime and Corruption Reporting Project (OCCRP), one of the 17 media partners involved in the global Pegasus investigation, out of the 1,000 phone numbers from Azerbaijan, the project researchers were so far able to identify 245 numbers that were targeted, one-fifth of which belonged to reporters, editors, or media company owners. The list also includes activists and their family members.

The new investigation also notes that:

> "The Citizen Lab's ongoing internet scanning and DNS cache probing has identified at least two suspected Pegasus operators in Azerbaijan that they call "BOZBASH" and "YANAR." According to the Citizen Lab, The YANAR Pegasus operator appears to have exclusively domestic-focused targeting within Azerbaijan, while the BOZBASH operator has targets including a broad range of entities within Armenia."

The NSO Group

NSO Group was set up in Israel in 2010 by Niv Carmi, Shalev Hulio, and Omri Lavie. On its website, the company claims to develop technology "to prevent and investigate terror and crime." But the surveillance technology appears to have been used against dissidents,

journalists, and activists across the world.

"NSO Group insists that it sells its software only to governments, suggesting that the clients in these countries represent intelligence services, law enforcement agencies, or other official bodies," the OCCPR has noted. Citizen Lab investigations reveal that NSO's Pegasus was used against dissidents at least since 2016 in numerous countries.

In 2019, the company came under fire when accusations emerged that it was infecting users' devices with malware by hacking WhatsApp. In response, WhatsApp and its parent company Facebook (now Meta) sued the NSO Group. In July 2020, a U.S. federal court judge ruled that the lawsuit against NSO Group could proceed despite the company's defense that "its business dealings with foreign governments, granted it immunity from lawsuits filed in U.S. courts under the Foreign Sovereign Immunity Act (FSIA)." In December 2020, Microsoft, Google, Internet Association, GitHub, and LinkedIn joined as parties in Facebook's [Meta's] ongoing legal battle against NSO. The most recent hearing took place in April 2021 and according to the news site Politico, the NSO Group appeared "unlikely to prevail."

Josh Gerstein, Politico's Senior Legal Affairs Reporter, noted:

> Even if the firm's effort to head off the suit fails, it could continue to fight the case in the trial court, but will likely be forced to turn over documents about its development of Pegasus and make executives available for depositions.

In April of this year, nine international human rights and press freedom organizations penned a letter to Chaim Gelfand, Vice-President for Compliance at NSO Group, asking the company "to deliver on its commitments to improve transparency about sales of its advanced spyware, and due diligence to protect human rights." The letter also rejected the NSO Group's claims "of their unverified compliance with human rights standards."

Ron Deibert, Director of the Citizen Lab at the University of Toronto, considers NSO's claims that they adhere to human rights standards to be "pure theater."

> The spectacle might be a mildly entertaining farce were it not for the very real and gruesome way in which its spyware is abused by the world's worst autocrats. NSO's irresponsible actions have proven their words are nothing more than hand-waving distractions from the harsh reality of the unregulated marketplace in which they, and their owners, thrive and profit.

Two years ago, the then-UN special rapporteur on freedom of expression, David Kaye, called for a moratorium on the sale of NSO-style spyware to governments until viable export controls could be put in place. Despite Kaye's warnings, the sale of surveillance software continued without any transparency or accountability.

The most recent investigation not only brings the company to the spotlight but also highlights the importance of control mechanisms imposed on spyware companies. The authors of the new investigation go further, concluding that despite the scandals, lawsuits, and sanctions, "NSO Group continues to ignore how its technology is used in violation of human rights to target civil society, including journalists and human rights defenders."

In a comment to Global Voices, Natalia Krapiva, the Tech-Legal Counsel at Access Now said:

> "This investigation is key to understanding the full scope of harms of invasive Pegasus spyware and the entire industry which has been operating with little to no oversight for years. We have seen Pegasus used to intimidate the free press, destroy the civic space, silence dissidents, undermine democracy, suppress independence movements, and more. Now we have evidence of Pegasus being used against civil society and humanitarian actors in a major international military conflict between Azerbaijan and Armenia. I am confident that our report will lead to more research and investigations as well as legal cases to bring accountability to the NSO, the spyware industry, and states who use these invasive technologies to attack human rights and humanitarian actors, journalists, and regime critics."

At the time of writing, no official statements on the investigation have yet been made in Azerbaijan. On May 25, leaders of Armenia and Azerbaijan were meeting in Moscow to discuss final peace agreement.

*

Note to readers: Please click the share button above. Follow us on Instagram and Twitter and subscribe to our Telegram Channel. Feel free to repost and share widely Global Research articles.

Featured image is by Waldemar. Free to use under Unsplash License.

Articles by: Arzu Geybullayeva