Media Diversity Institute

PEGASUS.
TARGETING ARMENIA
Report

Sargis Harutyunyan

Yerevan
2024

PEGASUS: TARGETING ARMENIA

Report

Sargis Harutyunyan

CONTENTS

Preface

Cybersecurity specialists in Armenia have determined that from mid-2020 to late 2023, several hundred individuals, including those in government, politics, economics, civil society, and the media, have received Apple threat notifications, which indicates that they were likely targeted by mercenary spyware.

Key figures such as now President Vahagn Khachaturyan, Prime Minister Nikol Pashinyan, and National Assembly Speaker Alen Simonyan, sometimes along with their families, also stated that they received Apple threat notifications.[1] [2] [3]

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 in May 2023 publicized 12 cases, where recipients of Apple threat notifications had their iPhones forensically tested and researchers found that they were attacked by Pegasus spyware. Notable, those attacks coincided with the 44-day war initiated by Azerbaijan against Nagorno-Karabakh and Armenia and subsequent military actions, marking the first known instance of a commercial spyware being deployed during wartime.[4]

The aim of this document is to provide a general overview of the deployment of the Pegasus mercenary spyware in Armenia to the broader populace and policymakers.

---

[1] Armenian Cabinet member, opposition MP among possible Pegasus spyware targets. Armenpress. Published November 25, 2021. Accessed June 18, 2024. https://armenpress.am/en/article/1069104

[2] Apple նոր մեյլեր ա ուղարկում: Pegasus... - Samvel Martirosyan. Facebook.com. Published 2023. Accessed June 18, 2024. https://www.facebook.com/samvel/posts/pfbid02mb9FeTTK1SHB3g3K3f6Ctm8c1S2pQRQC6GnbaPUdNkVfuLwQJ5jAg1mdYA8Qa46Yl.

[3] Արտակ Խուլյան. Փաշինյանը կտրականապես հերքում է կառավարության կողմից լրտեսական ծրագիր օգտագործելու մասին տեղեկությունը. "Ազատ Եվրոպա/Ազատություն" ռադիոկայան. Published March 15, 2023. Accessed June 18, 2024. https://www.azatutyun.am/a/32319719.html .

[4] Spyware in warfare: Access Now documents first-time use of Pegasus tech in Azerbaijan-Armenia conflict - Access Now. Access Now. Published May 25, 2023. Accessed June 18, 2024. https://www.accessnow.org/press-release/spyware-warfare-pegasus-in-azerbaijan-armenia-conflict/.

The Pegasus Scale

Pegasus is a spyware produced and sold by an Israeli firm NSO Group. Pegasus exploits security vulnerabilities in mobile devices to gain unauthorized access, often with no interaction (or clicks) by the user. Once installed, Pegasus allows the attacker to gain access to the victim's passwords, contact lists, calendar events, text messages, calls, and even to turn on the phone's camera and microphone to capture activity in the phone's vicinity.

While the full extent of the Pegasus spyware's reach remains undisclosed, insights from various expert analyses and journalistic inquiries over recent years provide some perspective on its impact.

In a 2016 report, the Citizen Lab at the Munk School of Global Affairs at the University of Toronto (the Citizen Lab), for the first time uncovered that Pegasus spyware was used to target UAE human rights advocate Ahmed Mansoor.[5]

In their 2018 report, the Citizen Lab revealed that the NSO Group's surveillance software may have been operational in 45 nations globally. Within the post-Soviet sphere, it specifically identified four Central Asian states: Kazakhstan, Kyrgyzstan, Uzbekistan, and Tajikistan as users[6].

By July 2021, the report called the Pegasus Project by Amnesty International and a consortium of media outlets, including Le Monde, The Guardian, Süddeutsche Zeitung, and The Washington Post, led by Forbidden Stories, indicated that the tally of Pegasus-utilizing countries had surpassed 50.[7] The organizations obtained around 50,000 phone numbers that they believe were selected as potential targets by Pegasus across various nations, with Azerbaijan also cited in these findings.[8] The Pegasus Project list contained the numbers of at least 3 sitting presidents, 10 prime ministers, 1 monarch, over 600 senior government officials and influential political personalities, 65 international business leaders, 85 notable human rights activists, and 189 journalists worldwide.[9]

---

[5] https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/.

[6] Marczak B. HIDE AND SEEK: Tracking NSO Group's Pegasus Spyware to Operations in 45 Countries - The Citizen Lab. The Citizen Lab. Published September 18, 2018. Accessed May 20, 2024. https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[7] The Pegasus Project: How Amnesty Tech uncovered the spyware scandal - new video. Amnesty International. Published March 23, 2022. Accessed July 1, 2024. https://www.amnesty.org/en/latest/news/2022/03/the-pegasus-project-how-amnesty-tech-uncovered-the-spyware-scandal-new-video/.

[8] About The Pegasus Project | Forbidden Stories. Forbiddenstories.org. Published 2021. Accessed May 20, 2024. https://forbiddenstories.org/about-the-pegasus-project/.

[9] Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses. Carnegieendowment.org. Published 2023. Accessed May 20, 2024. https://carnegieendowment.org/research/2023/03/why-does-the-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses?lang=en.

NSO Group's financial trajectory is telling as well. The firm's revenue was $40 million in 2014[10] with a workforce of around 50.[11] Annual revenue in 2018 was nearly six times that, at $250 million[12], and its staff count had ballooned to 700 by 2019[13].

Specific pricing details for Pegasus usage are not publicly available, which experts attribute to the secretive nature of the contracts and operations involved. Consequently, costs are negotiated on a case-by-case basis.

For instance, The New York Times reported in September 2016 that infecting 10 iPhones could cost $650,000, with an additional $500,000 required to set up the necessary supporting infrastructure tailored to the client's needs.[14]

Notably, NSO Group's contracts have been substantial, such as a $20 million agreement with the Mexican government in 2012 and a $55 million deal with Saudi Arabia in 2017[15], and in 2017 with Saudi Arabia - 55 million dollars[16].

[10] Brewster T. Everything We Know About NSO Group: The Professional Spies Who Hacked iPhones With A Single Text. Forbes. Published August 30, 2016. Accessed May 20, 2024. https://www.forbes.com/sites/thomasbrewster/2016/08/25/everything-we-know-about-nso-group-the-professional-spies-who-hacked-iphones-with-a-single-text/?sh=6ae2815e3997.

[11] Davies V. Who are NSO Group, the company being sued by Apple? Cybermagazine.com. Published November 25, 2021. Accessed May 20, 2024. https://cybermagazine.com/cyber-security/who-are-nso-group-company-being-sued-apple.

[12] NSO founders, management buy stake in firm from Francisco Partners. Timesofisrael.com. Published 2019. Accessed May 20, 2024. https://www.timesofisrael.com/nso-founders-management-buy-stake-in-firm-from-francisco-partners/.

[13] The Battle for the World's Most Powerful Cyberweapon, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

[14] How Spy Tech Firms Let Governments See Everything on a Smartphone, https://www.nytimes.com/2016/09/03/technology/nso-group-how-spy-tech-firms-let-governments-see-everything-on-a-smartphone.html.

[15] Who are NSO Group, the company being sued by Apple?, https://cybermagazine.com/cyber-security/who-are-nso-group-company-being-sued-apple.

[16] The Battle for the World's Most Powerful Cyberweapon, https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html.

Armenia Targeted

Armenian iPhone users started receiving Apple threat notifications from November 2021.[17] According to Apple, they are "designed to inform and assist users who may have been individually targeted by mercenary spyware attacks."[18] The language in Apple's notifications does not indicate what attacker or technology the company detected, which requires additional analysis.[19]

In other words, Apple notifications can mean Pegasus, Predator, Candiru or any number of other spyware attacks. This also means that it is not possible to determine the precise scope of Pegasus-related breaches in Armenia, simply based on how many people received Apple threat notifications. The full scale of NSO's customers also remains undisclosed due to the classified nature of these espionage activities conducted by intelligence agencies. However, Armenian cybersecurity specialists estimate that the number of individuals attacked by Pegasus spyware could be in the hundreds.

The only forensically confirmed cases of Pegasus spyware in Armenia are described in the 2023 joint investigation by Access Now, the Citizen Lab, CyberHUB-AM, and Ruben Muradyan, documenting Pegasus targeting of 12 civil society members in Armenia. However, to this date, there has been no comprehensive data or findings from Armenian state or law enforcement investigations made available, assuming such inquiries have taken place.

To bridge this information gap, this report also draws on insights from interviews with Armenian cybersecurity specialists, including Artur Papyan, co-founder of CyberHUB-AM, and Ruben Muradyan, an independent IT security expert, who have been researching the scope of the potential Pegasus targetings in Armenia.

Initial Strikes: July 2020

Research carried out by CyberHUB-AM and Ruben Muradyan into targeted smartphones in Armenia revealed that the initial successful infiltrations occurred no later than July 2020. This timeframe aligns with the Tavush skirmishes, during which, from July 12 to 21 of that year, hostilities erupted between the Armenian and Azerbaijani military forces in the Tavush region of Armenia.

This correlation is significant because subsequent analyses of infection data and Apple notifications indicated heightened Pegasus activity targeting Armenians during periods of

[17] https://support.apple.com/en-us/102174.
[18] ibid.
[19] Access Now's Digital Security Helpline and Apple threat notifications - Access Now. Access Now. Published May 2, 2024. Accessed July 3, 2024. https://www.accessnow.org/help/access-nows-digital-security-helpline-and-apple-threat-notifications/.

tension between Armenia and Azerbaijan, such as wars, border skirmishes, and negotiations between the parties. These patterns suggest possible Azerbaijani governmental involvement in the cyberattacks against Armenian targets.

Prior to this, Azerbaijan had engaged with the Italian HackingTeam[20] and Israeli Candiru[21]. The Carnegie Endowment for International Peace notes that Azerbaijan has been utilizing such surveillance tools since 2009, likely in reference to its collaboration with HackingTeam, established in 2003.[22]

It's likely that dissatisfaction with the outcomes from HackingTeam and Candiru led Baku to transition to Pegasus, or perhaps the capabilities offered by the NSO Group were more comprehensive and appealing.

Armenian Leadership in the Crosshairs

Armenia's Prime Minister Nikol Pashinyan[23], National Assembly Speaker Alen Simonyan[24], and President Vahagn Khachaturyan[25] have all publicly stated that they have received Apple notifications. At this point we have no forensic analysis as to what type of spyware the country's leadership was targeted with or if they were indeed targeted, or not.

Our fieldwork has confirmed that over 200 two hundred iPhones of various former and acting state officials, MPs, experts, civil society figures and journalists received Apple Threat Notifications. This is the largest collection of cases of known recipients of Apple Threat Notifications ever assembled.

Artur Papyan said in the interview, "Prime Minister Nikol Pashinyan, Speaker Alen Simonyan, and President Vahagn Khachaturyan have all claimed that they were spyware targets. Similar announcements came from the former National Security Service chief Artur

---

[20] Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

[21] So strategic relations with Azerbaijan became a family affair for Lieberman https://detaly.co.il/tak-strategicheskie-otnosheniya-s-azerbajdzhanom-stali-semejnym-delom-libermana/.

[22] Why Does the Global Spyware Industry Continue to Thrive? Trends, Explanations, and Responses, https://carnegieendowment.org/2023/03/14/why-does-global-spyware-industry-continue-to-thrive-trends-explanations-and-responses-pub-89229.

[23] Արտակ Խուլյան. Փաշինյանը կտրականապես հերքում է կառավարության կողմից լրտեսական ծրագիր օգտագործելու մասին տեղեկությունը. "Ազատ Եվրոպա/Ազատություն" ռադիոկայան. Published March 15, 2023. Accessed July 2, 2024. https://www.azatutyun.am/a/32319719.html

[24] Apple նոր մեյլեր ա ուղարկում՝ Pegasus... - Samvel Martirosyan. Facebook.com. Published 2023. Accessed July 2, 2024. https://www.facebook.com/samvel/posts/pfbid02mKyGhkhYv57vGtpXCSBALNWSptorDkJiADceDCz3RDWgvt558pJ7JjNNTezEx2Eel.

[25] Armenpress. Armenian Cabinet member, opposition MP among possible Pegasus spyware targets. Armenpress. Published November 25, 2021. Accessed July 2, 2024. https://armenpress.am/en/article/1069104.

Vanetsyan[26], ex-State Control Service head Davit Sanasaryan[27], and former Human Rights Defender Kristine Grigoryan—individuals privy to highly sensitive data.[28] Opposition members Davit Khazhakyan, Ruben Melikyan, and Samvel Farmanyan also were tested positive for Pegasus.[29]"

Over a dozen recipients of Apple Threat Notifications are members of Armenia's Security Council, Ministries of Foreign Affairs and Defense, National Security Service, and the Police.

Ruben Muradyan, who participated in the 2023 investigation, said in the interview with CyberHUB, "The Ministry of Foreign Affairs' staff was extensively compromised. The scale was immense; anyone potentially holding information on Armenia's security and foreign policy was a target. For instance, Anna Naghdalyan's phone underwent Pegasus infection 27 times, as iPhones require re-infection with Pegasus after each restart."

Muradyan's words are further backed by the Technical Brief[30] of Pegasus infections in Armenia published by CitizenLAB in May 2023, where more details about the targeting infrastructure and exploits used can be found.

Tallying the Pegasus Incursions

Regarding the scope of Pegasus's targeting in Armenia since July 2020, the precise success rate remains undisclosed, partly due to the factors mentioned earlier.

Most of the published findings come from the joint investigation by AccessNow, Citizen Lab, Amnesty International, CyberHUB-AM, and Ruben Muradyan. These findings suggest that between 2020-2021, Pegasus successfully compromised 12 individuals within Armenian civil society.[31]

The figures provided by Armenian experts suggest that the total number of cases of targeting (and thus some rate of presumed infection success) is likely to be significantly higher. Data

---

[26] Artur Vanetsyan - Այսօր Apple ընկերությունից նամակ ստացա, որն... Facebook.com. Published 2023. Accessed July 2, 2024. https://www.facebook.com/avav111/posts/pfbid0ho6NbY5QtJho24pCsfSEvvGX2TvCurfnKGr25Apd54VAUYdV7jqUeh8kyUUBaR4Hl.

[27] Երեկ գիշեր ժամը 2-ին Apple-ի... - Davit Sanasaryan. Facebook.com. Published 2023. Accessed July 2, 2024. https://www.facebook.com/sanasaryan/posts/pfbid0HnLVguwbPUiB2fo948RqwBYz7mevJUpscbhqvLgMZJ1MWcRCXx3Duh4ExAiaCK8Yl.

[28] Armenia spyware victims: Pegasus hacking in war. Access Now. Published November 27, 2023. Accessed July 2, 2024. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.

[29] Armenia spyware victims: Pegasus hacking in war. Access Now. Published November 27, 2023. Accessed July 2, 2024. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.

[30] Scott-Railton J. Armenia-Azerbaijan conflict: Pegasus infections - Technical Brief [1] - The Citizen Lab. The Citizen Lab. Published May 25, 2023. Accessed July 3, 2024. https://citizenlab.ca/2023/05/cr1-armenia-pegasus/.

[31] Armenia-Azerbaijan conflict Pegasus infections - Technical Brief, https://citizenlab.ca/2023/05/cr1-armenia-pegasus/. Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict, https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/.

from CyberHUB-AM and Ruben Muradyan indicate that since 2020, at least 200 individuals who received Apple notifications have sought their assistance.

It's important to note that this data pertains solely to the iOS operating system, as Google does not alert Android users about spyware targeting attempts. Thus, the total number of cases is likely to be even higher.

Researchers actively investigating this espionage software assert that from July 2020 onwards, Pegasus has likely targeted several hundred (as estimated by Artur Papyan) devices in Armenia. This takes into account the broad spectrum of targets, which included not only high-ranking officials but also rank-and-file employees, members of various state bodies, political groups, business representatives, civil society, journalists and media personnel.

The analysis of cyber attacks targeting Armenia reveals a clear pattern: the surge in such incidents has frequently coincided with periods of heightened tensions in Armenian-Azerbaijani relations. This includes events like the Tavush clashes in 2020, the 44-day war, military operations against Nagorno-Karabakh by Baku, border skirmishes, critical junctures in bilateral negotiations, and significant domestic political events within Armenia, such as the snap parliamentary elections in June 2021.

BOZBASH Is Following You

In the aftermath of a cyber-attack, the immediate question that arises for the victims is the identity of the perpetrator. Understanding who is responsible sheds light on the motives behind the attack, the specific reasons for being targeted, the type of information sought, the timing, and the appropriate countermeasures to be taken.

Initially, there was speculation among Armenian experts about whether domestic authorities were deploying Pegasus within the country, particularly against opposition politicians.[32] However, subsequent evidence pointed more strongly towards Azerbaijan. In May 2023, a comprehensive investigation jointly conducted by Access Now, CitizenLab, Amnesty International's Security Lab, CyberHUB-AM, and independent expert Ruben Muradyan was released, revealing Azerbaijan's role in the cyber espionage against Armenia using Pegasus.[33]

More specifically, the Technical Brief[34] published by CitizenLab disclosed that Azerbaijan had established at least two Pegasus command centers, referred to as Yanar and Bozbash,

[32] According to Ruben Muradyan, there have been several dozen cases of Pegasus targeting people representing the circle of the second and third Presidents of Armenia.
[33] Armenia-Azerbaijan conflict Pegasus infections - Technical Brief, https://citizenlab.ca/2023/05/cr1-armenia-pegasus/.
[34] Scott-Railton J. Armenia-Azerbaijan conflict: Pegasus infections - Technical Brief [1] - The Citizen Lab. The Citizen Lab. Published May 25, 2023. Accessed July 3, 2024. https://citizenlab.ca/2023/05/cr1-armenia-pegasus/.

by late 2018 or earlier (Note: this is CitizenLab's naming). Yanar was tasked with domestic operations, while Bozbash was designated for both domestic and international assignments, including those in Armenia.

It has been reported that over a thousand smartphones in Azerbaijan were targeted by these operations.[35]

[35] Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict, https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/.

Final Remarks

Looking ahead, it's likely that the occurrence, scope, and complexity of cyber attacks will escalate as our reliance on smartphones and various gadgets intensifies. Google's Threat Analysis Group disclosed in a recent February report the existence of approximately 40 commercial entities that provide surveillance services.[36]

Simultaneously, smartphone vendors and makers of mobile apps, like Apple, Google, WhatsApp, and Signal, have partnered with governments, malware researchers and human rights groups, to combat commercial spyware.[37] Several detection tools and techniques have become available[38], yet it's time to acknowledge a fundamental truth: the mobile phone is the world's most effective surveillance agent, so it will always be targeted.

[36] Buying Spying: Insights into Commercial Surveillance Vendor, https://storage.googleapis.com/gweb-uniblog-publish-prod/documents/Buying_Spying_-_Insights_into_Commercial_Surveillance_Vendors_-_TAG_report.pdf.

[37] It is well known that local human rights defenders, representatives of civil society, and journalists are among the primary targets of governments, especially in dictatorial countries, and such programs are used to spy on them.

[38] In July 2021, Amnesty International introduced the Mobile Verification Toolkit (MVT), a tool for detecting similar spyware on iOS and Android-based smartphones (https://docs.mvt.re/en/latest/). For iOS devices, the iMazing tool is available (https://imazing.com/guides/detect-pegasus-and-other-spyware-on-iphone).

Media Diversity Institute

www.mdi.am