ARMENIA

Digital Threat Landscape: Civil Society & Media

Internews
Local voices. Global change.

CyberHUB

Table of Contents

Background

Pegasus spyware has been used to target several politicians and civil society organizations in Armenia throughout the past year. Experts have identified links between these incidents of Pegasus and Azerbaijan's government, representing the first instance of Pegasus within the context of international conflict. The territorial dispute between Armenia and Azerbaijan is central to the governing of both countries and has led to multiple wars. While media coverage of Armenia's cyberthreat landscape focuses predominantly on spyware, civil society organizations face a plethora of other digital threats.

This report was prepared by Internews' Internet Freedom & Resilience team under a stream of work which strengthens civil society organizations (CSOs), journalists, and other human rights defenders (HRD) ability to detect, analyze, and build resilience to digital attacks through localized expertise in threat analysis and incident response. This report provides an overview of the threats faced by civil society and journalists in Armenia and guidance for digital safety experts supporting this community. It also provides context for the cybersecurity industry which may need to analyze security incidents affecting Armenian civil society and journalists. We conclude with a discussion of mitigation measures that can be proposed by digital security experts to the organizations, communities, and individuals with whom they work.

This report was written in close collaboration with CyberHub-AM, a Computer Emergency Response Team (CERT) for Armenian civil society, including NGOs, Human Rights Defenders, Activists, journalists, and independent media. They serve as a contact point and help desk for the above-mentioned groups in Armenia and collect, analyze, and anonymously and responsibly share incident data and indicators with the global threat intelligence community where appropriate.

The threats, trends and case studies highlighted in this report were identified through direct digital safety support for at-risk communities (provided by Internews and CyberHub-AM), desk research and conversations with trusted members of the Internet Freedom community. This report aggregates data from incident response work and documents attack patterns specific to Armenia.

October 2023

Written and Edited: Martijn Grooten, Ashley Fowler, Marc Shaffer, and Skyler Sallick
Copyediting, Design, and Layout: Skyler Sallick

Digital Threat Landscape

Political Context, Civil Society, and the Media

Following its independence from the USSR, Armenia has had an ongoing territorial conflict with Azerbaijan, resulting in multiple armed conflicts. The conflict revolves around an area referred to as Artsakh by Armenians and as Nagorno-Karabakh by the international community. The Nagorno-Karabakh region was recently invaded by Azerbaijan, resulting in the mass migration of the region's ethnically Armenian population.[1]

The First Nagorno-Karabakh War was fought between 1988 and 1994 until a Russian negotiated ceasefire. Under this agreement, Armenia controlled most of the Nagorno-Karabakh territory, but the lingering tension has been considered a root cause of economic issues in both Armenia and Azerbaijan. In 2020, another full-scale war broke out over the Nagorno-Karabakh territory, lasting six-weeks until the combatants agreed to a new ceasefire. This ceasefire, however, is viewed as a defeat by many Armenians.

In September 2023, Azerbaijan launched a full-scale invasion of the region, and, within 24 hours, Armenian forces in Nagorno-Karabakh surrendered control. Following this military action, over 100,000 ethnic Armenians fled the region, leading to a largescale refugee crisis.

As of the writing of this report in October 2023, the situation in Armenia is rapidly changing. In September 2023, Azerbaijan launched a full-scale invasion of the region, and, within 24 hours, Armenian forces in Nagorno-Karabakh surrendered control. Following this military action, over 100,000 ethnic Armenians fled the region, leading to a largescale refugee crisis.[2] At the time of writing, many remain fearful that Azerbaijan will continue their aggression and launch an invasion of southern Armenia. However, Azerbaijan's government denies the potential for this escalation. Azerbaijan has called on Armenia to peacefully establish a corridor that allows access to the Azerbaijani Nakhichevan exclave. Azerbaijan has previously threatened to establish this corridor with force. As a result of the invasion, the US Department of State has not renewed a waiver to the Freedom Support Act that allows the sale of weapons to Azerbaijan for the first time since 2002.[3]

While maintaining strong relations with Europe, Armenia also remains closely connected to Russia. Russian is the most widely spoken foreign language, and Russians do not require a visa to travel to the country. Russia also has a military base in Armenia – Russia's 102nd Military Base is located in Gyumri, Armenia and is under the command of the Southern Military District of the Russian Armed Forces. Russia also maintains a peacekeeping force based around the Armenia – Azerbaijan border and in the Nagorno-Karabakh region, although this peacekeeping force was significantly reduced as a result of the full-scale military invasion of Ukraine. Following this invasion, many Russian IT and tech workers, as well as some members of Russian civil society and journalists, moved to Armenia.[4] In 2022, Armenia abstained from voting on a UN resolution demanding Russia cease military activities and withdraw from Ukrainian territory.[5]

The failure of Russia to intervene following Azerbaijan's invasion of Nagorno-Karabakh has created uncertainty about the future of the Russian-Armenian relationship. Armenia additionally received no support from their membership in the Collective Security Treaty Organization (CSTO), leading to questions regarding the utility of membership. In October 2023, Armenia ratified the Rome Statute, and thus joined the International Criminal Court. Now, as a member of the ICC, Armenian authorities are obligated to arrest Russian president Vladimir Putin if he enters the country. Russia has voiced their staunch opposition to this move.[6]

Armenian civil society and media organizations are generally able to operate freely. However, there have been growing restrictions in recent years, and the situation may change as the regional context develops. Importantly, civil society played an active role in the 2018 protests that led to the change in government.[7] In 2021, the Armenian government implemented defamation laws that were used to prosecute journalists. However, domestic and international opposition led to their repeal in 2022.[8] Reporters without Borders reports that the Armenian government does not sufficiently protect freedom of the press, noting that violence against journalists often goes unpunished.[9]

These threats to free speech and the free operation of civil society groups are generally more present and damaging to already vulnerable communities. A recent criminal investigation highlights threats to free speech and civil society posed by discrimination against the Yazidi ethnic minority, the largest minority group in a largely ethnically homogeneous country. The government arrested Sashik Sultanyan, Head of the Yezidi Centre for Human Rights in Armenia, for inciting hatred and violence as a result of his activism for minority rights.[10] Armenia lacks an anti-discrimination law, and observers fear that this case will have a chilling effect on free speech more broadly.[11]

These threats to free speech and the free operation of civil society groups are generally more present and damaging to already vulnerable communities.

Armenia's LGBTQ+ community also faces widespread discrimination throughout the country, impacting the ability of civil society organizations to operate effectively.[12] Organizations working on behalf of the queer community, such as PINK Armenia and Right Side NGO, have faced intimidation, threats, and a judiciary that does not respond to homophobic violence.[13] Despite these threats, LGBTQ+ rights organizations continue to fight for change through engagement with the media sector and government, and by providing resources for queer Armenians.[14]

Cybersecurity in Armenia

Armenia was first connected to the Internet in 1994 with the introduction of the .am top-level domain. However, Internet usage in the country didn't fully take off until around 2010.[15] Armenia's close relationship with Russia has likely contributed to the freedom with which financially motivated hackers can live in the country. In 2013, Verizon reported that Armenia hosted a large number of these malicious actors, particularly compared to the size of the country.[16] In 2012, the alleged perpetrator of a large spam-sending Bredolab botnet, a Russian of Armenian descent, received a four year jail sentence from Armenian authorities.[17]

Armenia's police force reported a 20-25% growth trend in cybercrime between 2016 and 2018. Cybercrime in the country generally involves the theft of financial resources from the target, with the most common forms being bank transactions and theft from bank cards. Attackers target citizens through social media to steal banking details, often by impersonating a relative.[18] In 2019, an organized crime syndicate of Armenian and Indian nationality conducted a major tech support scam that targeted users in the United States and Canada.[19]

Users of the popular messenger applications Telegram and WhatsApp are often targeted in the country through scams and hacking attempts. Per conversations with the organization CyberHub-AM, messages with malicious intent are often written in Russian, and some targets may be "collateral damage" of campaigns attempting to target Russian nationals.

Because Telegram and WhatsApp are linked to the user's telephone number, anyone able to intercept SMS can take over an account if no passcode is set for extra protection. While this sometimes happens through targeted social engineering, account takeovers are commonly conducted without a clear motive. Additionally, many people who do not use WhatsApp report that their phone numbers have been used to set up a WhatsApp account, suggesting attackers have access to either the telecommunication company receiving the account verification SMS messages or to the entity platforms used to send them.

In recent years, state-sponsored digital attacks have been documented in Armenia. In 2019, the Russian-linked Turla group compromised four high profile Armenian websites in a "watering hole" attack,[i] two of which belonged to the government as documented by the cybersecurity company ESET.[20] Based on the group's previous activity and the websites compromised, Turla likely wished to target politicians and government officials in the attack.

In 2021, spyware designed by the Israeli spyware vendor Candiru targeted Armenians as part of a widespread campaign. The attacks relied on zero-day vulnerabilities[ii] in Microsoft software.[21] Politicians, human rights activists, and journalists were targets of this campaign. Around the same time, Google reported that targets in Armenia received emails with links exploiting zero-day vulnerabilities in Google Chrome.[22]

In a 2022 adversarial threat report, Meta reported on an Azerbaijani operation that involved malware and phishing, as well as fake accounts and websites.[23] Although largely deployed domestically, this attack also impacted some individuals in Armenia.

The State of Cybersecurity of Civil Society and Media

Civil society organizations and the media face the same attacks as all internet users in Armenia, but due to the nature of their work, they also face unique threats, and non-targeted attacks often have a larger impact. For an individual member of civil society, it is not always clear whether an attack was targeted or not. They frequently face threats to their Telegram, WhatsApp, and other social media accounts; website compromises; and DDoS attacks on their websites. An example

[i] In a watering hole attack, a website likely visited by a targeted community is hacked and infected with malware, to ensure the attack is targeted without the adversary having to reach out to the targets directly.

[ii] Zero-day vulnerabilities are vulnerabilities which at the time of use are unknown to the affected vendor.

of a website compromise impacting a civil society organization can be found in a case study below.

For an individual member of civil society, it is not always clear whether an attack was targeted or not. They frequently face threats to their Telegram, WhatsApp, and other social media accounts; website compromises; and DDoS attacks on their websites.

As is common around the world, many Armenian media organizations and other civil society groups operate with limited resources. They are making decisions that affect their digital security regularly. This includes running outdated software or downloading cracked, or unlicensed, software from the Internet rather than purchasing official software. The latter is so common that there are known cases of organizations who had licenses for official software and still downloaded a cracked version.[24]

One organization running cracked software was compromised by a digital attack; using this software allowed for the installation of a keylogger on the network, which in turn led to the takeover of the organization's Google account. It was only when Google warned about malware on the network that the compromise was detected.

Another NGO lost several thousand US dollars through a business email compromise (BEC) scam through which the organization's Yahoo account was hacked. The hackers used their access to social engineer an email convincing a donor to send funds to an attacker-created bank account. Though small scale in comparison to other BEC scams, the NGO was greatly impacted by the attack.[25]

Many of these threats can be traced to Azerbaijan-linked groups. For example, in October 2022, Azerbaijani hackers took over an Armenian hosting provider running outdated and vulnerable software, leading to a compromise of all the websites on it. Though not directly targeted to any individual customer, two of the websites belonged to local NGOs.[26] Turkish groups have also regularly targeted Armenian websites.

In addition to the less technically sophisticated attacks relying on weak digital security hygiene and social engineering that impact the whole country, some prominent Armenians, including members of civil society and journalists, have been targeted by two kinds of advanced Spyware: Predator and Pegasus.

In December 2021, Meta[27] and Citizen Lab[28] together first reported on Predator, a spyware developed by North Macedonia-based Cytrox. The report indicated that Armenia was one of the countries where Cytrox customers were based. Since then, CyberHub-AM has confirmed Predator infections on the devices of several "domestic political and media targets," leading to the suspicion that local security services are behind these attacks.[29]

Interestingly, compromised Telegram accounts were relied on to disseminate links that installed Predator, which could explain some of the more targeted account hijacking mentioned above. This is a clever technique: the accounts of low-to-medium risk individuals are generally easier to take over, while high risk individuals will find messages from these accounts –not realizing they are compromised – more credible and thus are more likely to click on the link.

The Pegasus spyware, developed and sold by Israel-based NSO Group, is the most (in)famous of its kind and has been the topic of many news articles, podcasts and even a book. Discovered in Mexico and the UAE in 2016, evidence of its use in Armenia first emerged in November 2021. At this time, Apple released notifications about nation-state activity targeting a select number of iPhone users. Though initial reports blamed the Armenian government, evidence suggests that the Azerbaijani government is behind the use of Pegasus in Armenia.[30]

The Azerbaijani government has acquired Pegasus and used the spyware to target local activists and journalists, demonstrating their capability of deploying the software in Armenia.

In 2023, CyberHub-AM, together with international partners, uncovered the use of Pegasus during the second Nagorno-Karabakh war, leading to even stronger suspicions of Azerbaijan as the perpetrator.[31] The Azerbaijani government has acquired Pegasus and used the spyware to target local activists and journalists,[32] demonstrating their capability of deploying the software in Armenia. For a case study about the use of Pegasus against a female journalist in Armenia, please refer to the case study.

Mitigation Measures

Account security is important for anyone in Armenia and for members of civil society and the media in particular. **Two-factor authentication is a must** – and mitigates the less controllable use of weak and/or reused passwords. Though better than no second factor at all, there is ample evidence that authentication via SMS is not secure enough in Armenia, especially for at-risk users. As an example, please see this report from CyberHub-AM, available in Armenian. Using an authentication app is better than SMS, and using a hardware token generally provides the best security, although this requires additional equipment.

Some messaging apps such as Telegram, WhatsApp, and Signal, require the use of a phone number to activate the account. Enabling two-factor authentication involves **adding a passcode** in addition to using SMS to access the account, providing security in cases of SMS compromise. When this feature is enabled, the app will periodically ask the user to input their passcode to ensure the messages are not being accessed by someone besides the owner of the account. This prevents account takeover through SMS interception, which is common in the country.

Endpoints, such as laptops and mobile phones, should be kept up to date by applying security patches to operating systems and other software whenever they become available. **Software should only be acquired from official sources**, which in many cases will require paying for it. NGOs should not be shy to discuss this with funders, or to look for free alternatives – either through open-source software or through programs that provide the software free of cost or at reduced prices to eligible NGOs.

Azerbaijani, and to a less extent Turkish, hackers commonly target websites of Armenian NGOs and civil society organizations with DDoS and defacement attacks. If such an attack could cause harm to an organization, they should take preventative measures, such as **utilizing a DDoS mitigation service** like Cloudflare or Project Shield for their website. Other than **ensuring the content management system running the website and its plugins are kept up to date**, they should **choose a hosting provider that consistently applies security patches** to its systems.

For websites and endpoints – such as laptops and mobile phones – alike, keeping **regular backups** allows users to recover data in the case it gets deleted, or in situations where a previous state needs to be recovered. Sometimes, hosting providers or device manufacturers automatically create backups, which is the most convenient option. If not, it is best to **create new backups weekly or at least monthly, ensure they work, and store them securely**, so that they themselves don't become a target.

Advanced spyware such as Pegasus and Predator commonly uses zero-day vulnerabilities and, especially in the former case, zero-click infections. That means a completely patched device can be infected in a way that a user cannot prevent using standard prevention methods, like not clicking suspicious links or attachments. This should be kept in mind by those at risk of such spyware.

Potential targets are urged to **use disappearing messages** on messaging apps, where messages are automatically deleted after a fixed amount of time. This can limit the damage of a future account compromise. Compartmentalization, by **using separate devices for work and personal use** or even **a separate device for high-risk work**, also limits the damage, but this comes with an obvious extra cost and inconvenience.

In addition to keeping phones up to date, **regularly rebooting iPhones**– once a day is a good idea – and **using Apple's Lockdown Mode** also mitigate the attacks.

Much less is known about spyware targeting Android, though that does not mean that Android users are less at risk. The more expensive Android devices are known to be more secure and usually have fixes for vulnerabilities available more quickly. Regularly rebooting a device also likely mitigates the damage as spyware doesn't persist beyond a reboot.[iii] Though in the case of Android, one should be aware that this may also remove evidence of a previous infection. For some users, this may be a concern.

Case Studies

Website Compromised Through Vulnerable WordPress Plugin

In May 2023, the website of an organization supporting minority rights in Armenia was compromised, with users being redirected to sites that were obvious scams and whose content was unrelated to that of the original website. Because the organization was preparing to publish an important report, the organization "felt" the compromise was targeted.

CyberHub-AM, a Computer Emergency Response Team (CERT) for Armenian civil society, including NGOs, human rights defenders, activists, journalists, and independent media, was called in to investigate the incident.

[iii] This is the case with all known iPhone spyware and likely also for Android spyware, especially the kind that 'roots' the device.

The affected organization's website runs on the popular open-source WordPress content management system, which NGOs and civil society organization around the world commonly use. Threat actors are often able to find and exploit vulnerabilities in WordPress and in particular its many plugins to take over websites and use them for malicious purposes or change their content, which is known as defacement.

During the investigation, CyberHub-AM looked for recently changed files on the web server and discovered various recently added or modified files belonging to a plugin called "posts-layouts." They also noted a new admin user "de-mouser-44" that was added to their WordPress account, confirming an outside actor had access to the account.

CyberHub-AM analyzed the path users were being redirected to after visiting the website and found that they were first redirected to cdn[.]scriptsplatform[.]com. The domain scriptsplatform[.]com had been registered only days earlier, on May 12th. This domain then redirected users to one of the scam websites, a common tactic in such infections.

By searching for the user added to the website, CyberHub-AM discovered there were many other websites that had been compromised in the same way. A quick check confirmed these sites also redirected to the scriptsplatform[.]com domain. Given that the other affected websites bore no relation to the organization in either content or geographical location, CyberHub-AM concluded that this was an opportunistic attack.

Checking the plugins the NGO had installed on the WordPress account, CyberHub-AM researchers found "Essential Addons for Elementor," an extension to the popular Elementor website builder plugin. In this plugin, a vulnerability had recently been found, suggesting this was the likely cause of the compromise.[33]

Shortly afterwards, the security firm Sucuri analyzed a campaign of mass infections exploiting this very vulnerability; the indicators of compromise in this report confirmed the Armenian organization was a victim of this campaign.[34]

CyberHub-AM removed a fake posts-layout plugin folder with malicious init.php, job.php files, as well as some obfuscated webshells. While cleanup was handled easily by CyberHub-AM, preventing the website from getting reinfected was not. Due to some dependencies, the Essential Addons for Elementor plugin could not be updated to patch the vulnerability without breaking essential functionality on the website.

This inability to update without breaking functionality, unfortunately, is common, especially for custom made websites. This shows that running such a website is an ongoing process requiring long-term maintenance. As CyberHub-AM writes in its post-mortem blog post, however, "most Armenian companies see their websites as a refrigerator that you buy and put in the kitchen and forget about it for years."[35]

Thankfully, the organization was scheduled to launch a new version of its website a few weeks after the incident, which would resolve the dependence issues. Until then, CyberHub-AM installed a web access firewall (WAF) to mitigate the risk of future threats. The website was not hacked again.

Pegasus Spyware Used to Hack Phone of Female Journalist

On November 10, 2022, Astghik Bedevyan received an email from Apple warning her that "state-sponsored attackers may be targeting [her] iPhone."[36] She was one of several people in Armenia who received this alert.

Bedevyan is a journalist with Radio Free Europe/Radio Liberty's (RFE/RL) Armenia service and Radio Azatutyun, a local media service. In 2020, she covered the Nagorno-Karabakh conflict and the 2021 snap parliamentary elections in Armenia which were heavily focused on that issue.[37]

Although Apple's threat notification did not say her iPhone had successfully been infected, she took the warning seriously and had her phone checked by CyberHub-AM, a Computer Emergency Response Team (CERT) for Armenian civil society, including NGOs, human rights defenders, activists, journalists, and independent media. Following CyberHUB-AM's advice, all members of RFE/RL's Yerevan bureau had their phones checked by Amnesty Tech. Amnesty Tech performed forensics on the phones and confirmed a successful Pegasus infection had taken place in 2021, around the time of the election. The phone of Bedevyan's RFE/RL colleague Karlen Aslanyan had also been breached.

The first evidence of Pegasus in Armenia was reported in 2021, when the spyware was found on the devices of several prominent politicians from both the government and the opposition.

Attackers had used Pegasus to infect the phones of a former ombudsman of the Republic of Artkash, a government spokesperson, and an academic.[38] A TV journalist and a prominent human rights defender were later discovered to have been infected as well. Several other victims chose to remain anonymous.

Although NSO Group – the Israeli company that developed the Pegasus software – only sells to governments, it is not possible to be 100% certain about the actor behind this campaign. In its report on the infections in Armenia, however, Amnesty International cites ample circumstantial evidence linking these infections to Azerbaijan.[39] Citizen Lab previously reported they believe there are two Pegasus operators in Azerbaijan, one domestic-focused and the other focused on Armenia.[40]

The Pegasus infection had a significant impact on Bedevyan. It did not just affect her work as a journalist; her phone also contained personal information, including information about her children. Bedevyan now knows that a foreign government likely had access to this information. "I felt that my personal privacy was rudely violated," she told Access Now.[41]

Analysis and reporting on Pegasus often overlooks the personal impact of Pegasus infections on victims, which is felt even more intensely by women and other vulnerable communities. The leak of a woman's personal information in Azerbaijan serves as a stark warning of the possible consequences of spyware collecting personal information in addition to professional. In 2020, the wife of a prominent government critic had her personal information – including her name, photos, and telephone number – published on social media and an escort website. Pro-government press then used this information to launch an attack campaign against her. Although the case has not been explicitly linked to Pegasus, evidence points to the information being stolen from her phone.[42]

Further Reading

As seen in this report, civil society organizations and journalists often face unique, advanced threats, while lacking the resources to detect, analyze and prevent them. An in-depth understanding of the threats facing civil society and media allows digital security practitioners to tailor their responses and better support the organizations they work with, leading to customized mitigation measures that are more effective and easier for civil society and media organizations to implement. For more information on the threats faced by civil society and journalists, Internews and their partners have authored the report "Global Trends in Digital Threats: Civil Society & Media," as well as Digital Threat Landscape Reports for Brazil, Mexico, Serbia, and Ukraine. These resources can be found on the Internews' Technology Resources webpage.

History of Armenia

The Republic of Armenia (Հայաստանի Հանրապետություն) is a unitary parliamentary republic located in the Armenian Highlands of the Caucasus region. The country is bordered by Turkey, Georgia, Azerbaijan, Iran, and Nakhchivan, an Azerbaijani exclave. Armenia has a long history going back to ancient times. In 301 AD, it was the first country that made Christianity the state religion.[43] The Armenian Apostolic Church is the national Church of Armenia today. The Armenian language is an Indo-European language with its own alphabet and no direct relatives.

Throughout most of its history, the territory where Armenians lived was part of foreign empires, in particular the Persian, Ottoman, and Russian ones. During the First World War, suspicion among the Ottoman government over Armenians volunteering in the Russian army led to the mass killing of 1 to 1.5 million Armenians. Though considered a genocide by most scholars, it remains a very controversial topic in Turkey, which does not recognize the genocide; this still strains relationships between Armenia and Turkey today.[44]

After a short-lived independent state, the country became part of the Soviet Union as the Armenian Soviet Socialist Republic and would remain so until it declared independence in 1991.[45]

Domestically, the government of Armenia was classified as having "soft authoritarian tendencies" by Freedom House, with a score of 45 out of 100 and a "partly free" ranking in 2017.[46] Following massive protests in 2018, the government was pressured to resign and replaced by a new administration that pledged to fight corruption and establish a more democratic system. As of the 2023 report, Armenia now has a score of 54 out of 100. The new government has faced several crises since taking power, including the outbreak of the COVID-19 pandemic, the second Nagorno-Karabakh War in 2020, and most recently the Azerbaijani seizure of Nagorno-Karabakh.[47]

Armenia is classified as an upper middle economy by the World Bank[48] and is increasingly geopolitically aligned with Europe despite its geographic location. Armenia is a member of the United Nations,[49] the Council of Europe,[50] and the World Trade Organization,[51] as well as several

Eurasian aligned organizations, such as the Commonwealth of Independent States,[52] the Asian Development Bank,[53] and the Collective Security Treaty Organization.[54]

Acknowledgements

Since 2021, Internews has worked with seven Threat Labs (*local organizations with the technical capacity and appropriate tools to analyze suspicious phishing and malware samples and then share information back to the community regarding attack trends, emerging threats, and countermeasures*) to respond to incidents affecting the digital security of civil society and media organizations around the world. The data collected through the incident response program helped shape mitigations and response approaches for at-risk communities and informed this report.

Internews would like to express our gratitude to the community of Threat Labs that worked with us on this project. They are committed to assisting those in need and ensuring that their partners in civil society and media organizations can complete their important work safely and effectively. In total, this project supported Threat Labs in responding to over 200 digital security incidents and publishing over 60 educational resources through their websites and social media platforms.

Special thanks to CyberHub-AM for providing the information to document and share these case studies and for reviewing and contributing valuable feedback to this report. The report would not have been possible without Yana Ghahramanyan, Samvel Martirosyan, and Artur Papyan.

Endnotes

[1] "Explainer: What is Nagorno-Karabakh and why are tensions rising?" *Al Jazeera*. April 24, 2023. https://www.aljazeera.com/news/2023/4/24/explainer-what-is-nagorno-karabakh-why-are-tensions-rising.

[2] Ertl, Michael. "Nagorno-Karabakh: Conflict between Azerbaijan and Armenians explained." BBC News. September 28, 2023.

[3] Bazail-Emil, Eric and Gabriel Gavin. "Blinken warned lawmakers Azerbaijan may invade Armenia in coming weeks." Politico. October 13, 2023. https://www.politico.com/news/2023/10/13/blinken-warned-lawmakers-azerbaijan-may-invade-armenia-in-coming-weeks-00121500.

[4] Amiryan, Tigran and Anna Sokolova. "Relocated Russian Democracy - A View from Armenia." Heinrich Böll Stiftung. June 1, 2022. https://ge.boell.org/en/2022/06/01/relocated-russian-democracy-view-armenia.

[5] Tatikyan, Sossi. "The Context Behind Armenia's UN Vote on Ukraine." *EVN Report*. March 3, 2022. https://evnreport.com/politics/the-context-behind-armenias-un-vote-on-ukraine/.

[6] Atasuntsev, Alexander. "Long-Standing Ties Between Armenia and Russia Are Fraying Fast." Carnegie Endowment for International Peace. October 13, 2023. https://carnegieendowment.org/politika/90768.

[7] "Freedom in the World 2023: Armenia." Freedom House. Accessed July 2023. https://freedomhouse.org/country/armenia/freedom-world/2023.

[8] Ibid.

[9] "Armenia." Reporters Without Borders. Accessed July 2023. https://rsf.org/en/country/armenia.

[10] "Armenia must drop 'intimidating' criminal charges against minority rights activist – UN experts." United Nations, OHCHR Press Release. August 10, 2021. https://www.ohchr.org/en/press-releases/2021/08/armenia-must-drop-intimidating-criminal-charges-against-minority-rights.

[11] Chilingaryan, Anahit. "High Stakes for Armenian Democracy in Rights Defender's Trial." Human Rights Watch. June 21, 2022. https://www.hrw.org/news/2022/06/21/high-stakes-armenian-democracy-rights-defenders-trial.

[12] "Public opinion toward LGBT people in Yerevan, Gyumri and Vanadzor cities." We and Our Rights. 2011. https://issuu.com/pinkarmenia/docs/lgbtsurveyen/9?e=3748946/2746746.

[13] "LGBT activist Mamikon Hovespyan announced as equality award winner for 2017." Equal Rights Trust. July 25, 2017. https://www.equalrightstrust.org/news/lgbt-activist-mamikon-hovespyan-announced-equality-award-winner-2017; Pilishvili, Catherine. "Another Change to Address Homophobic Violence in Armenia." Human Rights Watch. August 28, 2020. https://www.hrw.org/news/2020/08/28/another-chance-address-homophobic-violence-armenia.

[14] "LGBT activist Mamikon Hovespyan announced as equality award winner for 2017," Equal Rights Trust.

[15] Papyan, Artur. "Internet penetration rate has declined in Armenia in 2020 according to ITU." *The Armenian Observer Blog*. October 16, 2020. https://ditord.com/2020/10/internet-penetration-rate-has-declined-in-armenia-in-2020/.

[16] Ranum, Marcus J. "FUDwatch: Armenia." Tenable. May 3, 2013. https://www.tenable.com/blog/fudwatch-armenia.

[17] "Russian spam mastermind jailed for creating botnet." *BBC*. May 24, 2012. https://www.bbc.com/news/technology-18189987.

[18] "Armenia police warn of growing cybercrime rate." *Armenpress*. Last modified June 12, 2018. https://armenpress.am/eng/news/937066/.

[19] "Armenian police bust Yerevan-based cybercrime syndicate targeting U.S. users via tech support scam." *Armenpress.* Last modified May 1, 2019. https://armenpress.am/eng/news/973297.html.

[20] Faou, Matthieu. "Tracking Turla: New backdoor delivered via Armenian watering holes." We Live Security, ESET Research. March 12, 2020. https://www.welivesecurity.com/2020/03/12/tracking-turla-new-backdoor-armenian-watering-holes/.

[21] Marczak, Bill, John Scott-Railton, Kristin Berdan, Bahr Abdul Razzak, and Ron Deibert. "Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus." The Citizen Lab. July 15, 2021. https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

[22] Stone, Maddie and Clement Lecigne. "How we protect users from 0-day attacks." Google, Threat Analysis Group. July 14, 2021. https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/.

[23] Nimmo, Ben, David Agranovich, and Nathaniel Gleicher. "Quarterly Adversarial Threat Report." Meta. April 2022. https://about.fb.com/wp-content/uploads/2022/04/Meta-Quarterly-Adversarial-Threat-Report_Q1-2022.pdf.

[24] Information provided by CyberHub-AM.

[25] Information from incident response provided by CyberHub-AM.

[26] Information from incident response provided by CyberHub-AM.

[27] Dvilyanski, Mike, David Agranovich, and Nathaniel Gleicher. "Threat Report on the Surveillance-for-Hire Industry." Meta. December 16, 2021. https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.

[28] Marczak, Bill, John Scott-Railton, Bahr Abdul Razzak, Noura Al-Jizawi, Siena Anstis, Kristin Berdan, and Ron Deibert. "Pegasus vs. Predator: Dissident's Doubly-Infected iPhone Reveals Cytrox Mercenary Spyware." The Citizen Lab. December 16, 2021. https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/.

[29] "Review of Attacks Against Armenian Telegram Users in Recent Months." CyberHUB. Last modified August 26, 2022. https://cyberhub.am/en/blog/2022/08/26/review-of-attacks-against-armenian-telegram-users-in-recent-months/.

[30] "Arsen Babayan: How authorities infect victims' phones with Pegasus spyware." *Panorama*. Last modified November 27, 2021. https://www.panorama.am/en/news/2021/11/27/Arsen-Babayan/2604970.

[31] Krapiva, Natalia, and Giulio. "Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict." Access Now. May 25, 2023. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.

[32] RFE/RL. "Azerbaijan Suspected Of Spying On Reporters, Activists By Using Software To Access Phones." RadioFreeEurope RadioLiberty. Last modified July 18, 2021. https://www.rferl.org/a/azerbaijan-pegasus-spying-nso/31365076.html.

[33] Muhammad, Rafie. "Critical Privilege Escalation in Essential Addons for Elementor Plugin Affecting 1+ Million Sites." Patchstack. Last modified May 11, 2023. https://patchstack.com/articles/critical-privilege-escalation-in-essential-addons-for-elementor-plugin-affecting-1-million-sites/.

[34] Martin, Ben. "Vulnerability in Essential Addons for Elementor Leads to Mass Infection." *SucriBlog*. Las modified May 18, 2023. https://blog.sucuri.net/2023/05/vulnerability-in-essential-addons-for-elementor-leads-to-mass-infection.html.

[35] "Hackers leverage vulnerability of Essential Addons plugin to exploit Armenian WordPress sites." CyberHUB. Last modified May 23, 2023. https://cyberhub.am/en/blog/2023/05/23/hackers-leverage-vulnerability-of-the-essential-addons-plugin-to-exploit-armenian-wordpress-sites/.

[36] "Armenia: Azerbaijan Hacks Armenian Journalist Astghik Bedevyan's Phone During War." Coalition For Women in Journalism. May 29, 2023. https://www.womeninjournalism.org/threats-all/armenia-azerbaijan-hacks-armenian-journalist-astghik-bedevyans-phone-during-war.

[37] "Armenia PM Pashinyan's Civil Contract claims victory in snap poll." *Al Jazeera.* June 21, 2021. https://www.aljazeera.com/news/2021/6/21/armenia-nikol-pashinyan-claims-victory-in-snap-polls.

[38] Krapiva, Natalia, and Giulio. "Hacking in a war zone: Pegasus spyware in the Azerbaijan-Armenia conflict." Access Now. May 25, 2023. https://www.accessnow.org/publication/armenia-spyware-victims-pegasus-hacking-in-war/.

[39] "Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict." Amnesty International. May 25, 2023. https://www.amnesty.org/en/latest/news/2023/05/armenia-azerbaijan-pegasus-spyware-targeted-armenian-public-figures-amid-conflict/.

[40] Scott-Railton, John, Bill Marczak, Bahr Abdul Razzak, Nicola Lawford, and Ron Deibert. "Armenia-Azerbaijan conflict: Pegasus infections – Technical Brief [1]." The Citizen Lab. May 25, 2023. https://citizenlab.ca/2023/05/cr1-armenia-pegasus/.

[41] Krapiva, "Hacking in a war zone: Pegasus spyware in Azerbaijan-Armenia conflict."

[42] Patrucic, Miranda and Kelly Bloss. "Life in Azerbaijan's Digital Autocracy: 'They Want to be in Control of Everything.'" Organized Crime and Corruption Reporting Project. July 18, 2021. https://www.occrp.org/en/the-pegasus-project/life-in-azerbaijans-digital-autocracy-they-want-to-be-in-control-of-everything.

[43] "Armenia country profile." *BBC*. Last modified July 3, 2023. https://www.bbc.com/news/world-europe-17398605.

[44] Ibid.

[45] Ibid.

[46] "Freedom in the World 2017: Armenia." Freedom House. Accessed July 2023. https://freedomhouse.org/country/armenia/freedom-world/2017.

[47] "Armenia country profile," *BBC*.

[48] "Middle income." The World Bank, Data. Accessed July 2023. https://data.worldbank.org/country/XP.

[49] "Member States." United Nations. Accessed July 2023. https://www.un.org/en/about-us/member-states.

[50] "46 Member States." Council of Europe. Accessed July 2023. https://www.coe.int/en/web/portal/46-members-states.

[51] "Members and Observers." World Trade Organization. Accessed July 2023. https://www.wto.org/english/thewto_e/whatis_e/tif_e/org6_e.htm.

[52] "Commonwealth of Independent States." *Britannica*. Accessed July 2023. https://www.britannica.com/topic/Commonwealth-of-Independent-States.

[53] "Who We Are." Asian Development Bank. Accessed July 2023. https://www.adb.org/who-we-are/about.

[54] "Countries." Collective Security Treaty Organization. Accessed July 2023. https://en.odkb-csto.org/countries/.