www.mdi.com

Media Diversity Institute

CyberHUB

ARMENIA COUNTRY THREAT LANDSCAPE 2023

Spyware Accountability Initiative

published - 2024

www.cyberhub.am

Table of CONTENTS

INTRODUCTION

Armenia is notable in the context of digital security for several reasons. It has experienced state-sponsored cyberattacks, including the use of NSO Group's Pegasus spyware during the Armenia-Azerbaijan conflict in Nagorno-Karabakh. The geopolitical landscape is further complicated by the involvement of global cyber powers such as Russia, Iran, and Israel, with the latter providing services for Azerbaijan. These nations have been known to actively operate within Armenia, exacerbating the already tense cyber environment.

This report outlines the threats faced by civil society and journalists in Armenia, offering valuable insights for cybersecurity experts. Major technology companies like Google, Microsoft, Meta, and Apple have all issued reports highlighting various cyber-attacks targeting Armenia. These reports underscore the urgent need for enhanced cybersecurity measures to protect sensitive data and infrastructure.

Furthermore, Armenia has adopted a government-approved strategy focusing on innovative technologies, cybersecurity, and e-services as part of its digital transformation efforts. Despite systemic weaknesses, the country acknowledges the importance of cybersecurity in an increasingly interconnected world.

The rapid increase in cybercriminal activities has created an urgent need for Armenia to strengthen its cybersecurity frameworks and raise public awareness about the rising dangers online. Many cybercriminal groups use sophisticated methods and target both individuals and businesses, employing phishing, ransomware, and other malicious tactics. With these developments, the need for comprehensive national cybersecurity measures has become increasingly evident to counteract both domestic and foreign cyber threats.

INTRODUCTION

This report was prepared by the Media Diversity Institute's **CyberHUB-AM** team, with the support from the Spyware Accountability Initiative (SAI).

CyberHUB-AM is an IT support hub and a Threat lab for the Armenian civil society — NGOs, Human Rights defenders, activists, journalists and independent media. It serves as a point of contact and a help desk for the abovementioned groups in Armenia and collects, analyzes and, where appropriate, responsibly and anonymously shares incident data and threat indicators with the global threat intelligence community.

Media Diversity Institute – Armenia (MDIA) is a non-profit, non-governmental organization that seeks to leverage the power of the traditional media, social media and new technologies to safeguard human rights, help build a democratic, civil society, give voice to the voiceless and deepen the collective understanding of different types of social diversity. MDIA was established on April 18, 2006. Since 2018 MDIA has become more involved in Digital Security, technologies for exposing disinformation and misinformation and has provided IT audits, risk assessments, triage and security incident response to dozens of prominent Armenian Human Rights and media organizations, activists, journalists.

Armenia is a country under constant exposure to cyber threats of various levels. The geopolitical situation, the ongoing military conflict with Azerbaijan—backed militarily and politically by Turkey—the deteriorating relations with Russia, and numerous other factors make Armenian cyberspace a prime target for state-sponsored hacker groups from around the world. These threats come from multiple directions, aiming to exploit the vulnerabilities within Armenia's digital infrastructure, posing a serious security concern for the country.

Cybercrime also continues to grow in Armenia's digital landscape. Strangely enough, the escalation of the full-scale invasion of Ukraine, coupled with the significant influx of refugees from Russia to Armenia, has contributed to a surge in various types of cyber fraud. Different schemes of digital scams and fraudulent practices have migrated along with the relocating population from Russia and other post-Soviet countries, embedding themselves within Armenia's online environment.

The rapid increase in cybercriminal activities has created an urgent need for Armenia to strengthen its cybersecurity frameworks and raise public awareness about the rising dangers online. Many cybercriminal groups use sophisticated methods and target both individuals and businesses, employing phishing, ransomware, and other malicious tactics. With these developments, the need for comprehensive national cybersecurity measures has become increasingly evident to counteract both domestic and foreign cyber threats.

Armenia faces a unique challenge in navigating its cybersecurity due to its geopolitical context. The constant state of conflict, regional tensions, and changing alliances place Armenia in a vulnerable position, both physically and digitally. To counteract these threats, Armenia must

collaborate internationally to improve its cyber defenses, secure its critical infrastructures, and protect its citizens from the rising tide of cyber threats and attacks.

As a significant example of the threats that it faces -- in 2023, Armenia became one of the most discussed countries in digital security due to the discovery of Pegasus spyware used to target politicians, media, and civil society. The spyware has been linked to the government of Azerbaijan, and as such, represents the first instance of Pegasus being used in the context of international conflict. The ongoing disputes between Armenia and Azerbaijan have long been central to politics of both countries and led to war multiple times. While spyware has been central in media coverage, civil society in Armenia faces several other threats to their digital security.

Political Context, Civil Society, and the Media

While maintaining strong relations with Europe, Armenia remains closely connected to Russia. Russian is the most widely spoken foreign language in the country, and Russians can travel to Armenia visa-free. Russia also maintains a military presence in Armenia, including the 102nd Military Base in Gyumri and peacekeeping forces along the Armenia-Azerbaijan border and in the Nagorno-Karabakh region. Following Russia's invasion of Ukraine in 2022, a significant number of Russian IT and tech workers, as well as civil society members and journalists, relocated to Armenia. Despite these ties, Armenia found itself in a challenging position on the global stage; it abstained from voting on a UN resolution demanding Russia cease military activities and withdraw from Ukrainian territory.

The evolving geopolitical landscape has further complicated Armenia's security challenges. The ongoing

conflict with Azerbaijan, exacerbated by Turkey's military and political backing of Azerbaijan, has left Armenia vulnerable to both physical and digital threats. In 2023, Armenia became a focal point in digital security discussions due to the use of Pegasus spyware targeting its politicians, media, and civil society, marking the first instance of Pegasus being used in an international conflict. These developments underscore the urgent need for Armenia to enhance its cybersecurity measures and collaborate internationally to safeguard its digital infrastructure and protect its citizens from multifaceted security threats.

Civil society and media organizations are generally able to operate freely in Armenia, but there have been some restrictions in recent years. Civil society played a role in the 2018 protests that led to the change in government.[1] 2021 saw the implementation of defamation laws that were used to prosecute journalists, but outcry both domestically and internationally led to their repeal in 2022.[2] The lack of comprehensive anti-discrimination laws and the discrimination faced by ethnic minorities and the LGBTQ+ community further exacerbate the precarious state of civil liberties in Armenia.

Cybersecurity in Armenia

In 2018, the police reported a 20-25% rise in cybercrime over the past two years. Most cybercrimes involved theft, especially bank transactions and card fraud. Criminals often use social media to steal banking details.[3] In 2019 a major tech support scam targeted users in the United States and Canada, run by an organized crime syndicate of Indian and Armenian nationals.[4]

Telegram and WhatsApp are popular messengers in the country and their users are often targeted through scams and hacking attempts. Many messages with a malicious

intent are written in Russian and some may be 'collateral damage' of campaigns targeting Russians.

In 2021, people in the country were reported among the targets of a campaign by Israeli spyware vendor Candiru that used zero-days – vulnerabilities which at the time of use were unknown to the affected vendor.[5] Targets in this campaign included politicians, human rights activists, and journalists. Around the same time, Google reported that targets in the country had received emails with links exploiting zero-day vulnerabilities in Google Chrome.[6]

In a 2022 adversarial threat report, Meta reported on an operation from Azerbaijan that involved malware and phishing as well as fake accounts and websites.[7] The operation, aside from targeting many within Azerbaijan, also targeted some individuals in Armenia.

Earlier, in September 2023 ESET reported targeted attacks by the Russian APT 28 hacking group against governmental institutions in Ukraine, Armenia, and Tajikistan. In June 2023, ESET discovered a set of spearphishing campaigns, which we named Operation RoundPress, exploiting an XSS vulnerability in Roundcube. Using this vulnerability, attackers are able to inject malicious JavaScript code into the victim's Roundcube webmail server. The injected code is able to steal emails, address books, and create forwarding rules to steal incoming emails. According to ESET`s telemetry, Operation RoundPress targets government staff in Armenia, Tajikistan, and Ukraine. [**source**]

It should be noted that various Russian state affiliated groups, including Turla associated with FSB and Ember Bear group attributed to GRU, were active in Armenia. [**source**]

Many threats originate from Azerbaijan-linked groups. For instance, in October 2022, Azeri hackers compromised an Armenian hosting provider using outdated software, affecting all websites on it, including two owned by local NGOs. Turkish groups also frequently target Armenian websites.

next...

Threat Report

Mercenary Spyware

Phishing

DDoS

Website Hacks

RATs

Insider attacks

Mercenary Spyware

Mercenary spyware refers to sophisticated surveillance software developed by private companies and sold to governments or other entities, usually dealing with law enforcement. Unlike traditional state-sponsored spyware, mercenary spyware is commercially available and often used to target specific individuals, such as drug traffickers, terrorists, criminals. Investigations by the Citizenlab, Amnesty International, AccessNow, Forbidden Stories and others has revealed that mercenary spyware is often misused by targeting also political dissidents, journalists, human rights activists, and other high-profile figures. This type of spyware can exploit vulnerabilities in devices to gain unauthorized access to personal data, communications, and even control over the device's camera and microphone. Notable examples include the Pegasus spyware developed by the NSO Group, which has been used in numerous high-profile cases to conduct covert surveillance.

A joint investigation by Access Now, CyberHUB-AM, the Citizen Lab, Amnesty International's Security Lab, and independent researcher Ruben Muradyan published in May 2023[8] uncovered the use of NSO Group's Pegasus spyware against civil society in Armenia during the Azerbaijan-Armenia conflict. The investigation revealed that at least 12 individuals, including journalists, human rights defenders, and a United Nations official, were targeted with Pegasus spyware between October 2020 and December 2022.

The spyware infections were linked to significant events in the Nagorno-Karabakh conflict, such as the 2020 war, subsequent peace talks, and the ongoing blockade of the Lachin corridor. Victims included high-profile figures like Kristinne Grigoryan, the former Human Rights Defender of Armenia, and Anna Naghdalyan, a former spokesperson for Armenia's Foreign Ministry.

The investigation began after Apple notified users in November 2021 about potential state-sponsored spyware targeting. This led several Armenian civil society members to seek help from CyberHUB-AM and Access Now's Digital Security Helpline. Forensic analysis confirmed multiple infections, highlighting the extensive use of Pegasus spyware in this international conflict.

Phishing

Phishing is a type of cyber attack where attackers impersonate legitimate entities to deceive individuals into providing sensitive information, such as passwords, credit card numbers, or personal details. These attacks often occur through emails, messages, or websites that appear to be from trusted sources but are actually fraudulent. The goal is to trick victims into clicking on malicious links or downloading harmful attachments, leading to data breaches, financial loss, or identity theft. Phishing exploits human psychology, relying on urgency, fear, or curiosity to prompt quick, unthinking responses from the targets.

Throughout 2023, several organizations in Armenia fell victim to phishing attacks, highlighting the growing threat of cybercrime in the region.

The Women's Rights House of Gyumri was targeted by a phishing campaign that aimed to steal sensitive information by masquerading as legitimate communication. This attack disrupted their operations and raised concerns about the security of personal data held by the organization.

Similarly, the Pahapan Foundation experienced a phishing attack on Facebook, where attackers used fake messages to trick staff into revealing their login credentials. This breach allowed the attackers to gain unauthorized access to the Foundation's Facebook page, potentially

compromising sensitive information and damaging the organization's online presence.

The Women's Resource Center also faced a phishing attack on Facebook, where cybercriminals sent deceptive messages to staff members, leading to the compromise of their Facebook account. This incident not only disrupted their social media activities but also posed a risk to the privacy and security of their supporters and beneficiaries.

Shant TV, a prominent media outlet, was another victim of a phishing attack on Facebook. The attackers used sophisticated techniques to deceive employees into providing their login details, resulting in the temporary loss of control over their Facebook page. This incident highlighted the vulnerability of media organizations to cyber threats and the importance of robust cybersecurity measures.

Lastly, the Doctor's Union suffered a phishing attack that led to the loss of access to their Facebook page. The attackers sent fraudulent messages claiming to be from Facebook's support team, tricking the Union's staff into divulging their login credentials. This breach not only affected their online presence but also raised concerns about the potential misuse of sensitive information related to their members.

DDoS

A Distributed Denial-of-Service (DDoS) attack is a malicious attempt to disrupt the normal traffic of a targeted server, service, or network by overwhelming the target or its surrounding infrastructure with a flood of Internet traffic. This overload originates from multiple compromised systems (often referred to as a botnet) and can manifest in various forms, such as high-volume traffic

designed to consume bandwidth, or malformed packets intended to exploit vulnerabilities. The ultimate goal of a DDoS attack is to render the targeted resource unavailable to legitimate users.

Distributed Denial of Service (DDoS) attacks have become increasingly common in Armenia, particularly in the context of the ongoing Armenia-Azerbaijan conflict and internal political strife. These cyber attacks are often used as tools to suppress information and disrupt the operations of media outlets, civil society organizations, and governmental institutions. The high stakes and contentious nature of the conflict exacerbate the frequency and intensity of these attacks, making cybersecurity a critical concern for those involved.

On October 24th and 25th, Hraparak.am, a prominent Armenian opposition media outlet, experienced an aggressive Distributed Denial of Service (DDoS) attack. The attack began on October 24th, with the site receiving 1.5 billion requests over the span of 12 hours. The attackers subsequently identified amplification URLs and redirected their requests accordingly.

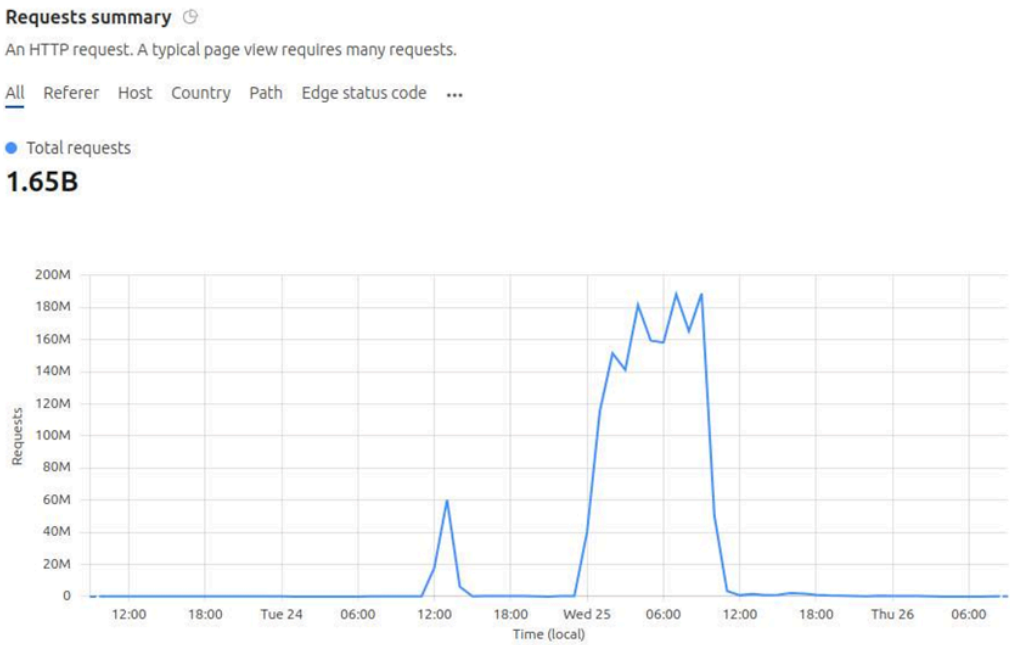
Hexens, a cybersecurity firm, responded to the incident at 12:40 on October 25th. Within 25 minutes, they managed to restore the site's functionality. The attack involved approximately 20,000 hosts, peaking at 200,000 requests per second, making it the second most powerful attack they had encountered.

The attackers demonstrated a high level of sophistication, altering their approach four times during the Incident Response. They discovered new amplification endpoints and adapted their methods; for instance, when GET requests were blocked by the rate limiter, they switched to POST requests.

The Hexens team believes that the attacks were triggered by the publication of several articles on Hraparak.am, which can be found at the following URLs:

- https://hraparak.am/post/a7aa0f305f471a553d5f6ec19f6c0268
- https://hraparak.am/post/a9108423851caa624ce4e13462f59379
- https://hraparak.am/post/692c7a3185d50d4cf00f21e3e9b4f4ad
- https://hraparak.am/post/787a0eeab6959761f81b18bbb386f1e8
- https://hraparak.am/post/dc49dcd5dbae94bf57b70f64b13bfa5a

In response to this incident, Hexens has offered to help independent media outlets defend against DDoS attacks free of charge. Special thanks to DigiFence for their support in this endeavor.



Website Hacks

During the 2023 several Azerbaijani hacking teams, including big community calling itself Anti-Armenian, reported defacements of hundreds Armenian web-sites.Among the others hackings of several media-outlets and CSO sites were reported, including news.am, yerkir.am, mamul.am, radiofama.am, transparency.am. Attacks were mostly on the days of military attack of Azerbaijan against Nagorno-Karabakh/Artsakh.

On a separate incident, in May 2023, the website of an organization supporting a marginalized community 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 compromise 'felt' 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.

The affected organization's website runs on the popular open-source WordPress content management system, which is widely used among NGOs and civil society organizations around the world. Vulnerabilities in WordPress and in particular its many plugins are commonly found and lead to websites being taken over and used for malicious purposes or having their contents changed ('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 'wp-demouser-44' that was added to WordPress, which confirmed someone else had access to the account.

Following the path users were being redirected to after visiting the website, it was noted that the first redirect was to cdn[.]scriptsplatform[.]com, with the domain scriptsplatform[.]com having been registered only days earlier, on May 12th. The domain would redirect users to one of the scam websites, which is common in such infections.

A search for the user that had been added showed there were many other websites that had been compromised in the same way. A quick check confirmed these sites also redirected to the same domain. Given that the other affected websites bore no relation to the organization in either content or geographical location, it became clear this was an opportunistic attack.

Checking the plugins that were installed, 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 so this was the likely caused of the compromise.[9]
Shortly afterwards, 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 very campaign.[10]

Cleaning up the infected website was easy; preventing the website from getting reinfected (by updating the Essential Addons for Elementor plugin) was not. Some dependencies prevented this update from being performed without breaking essential functionality on the website. This, unfortunately, is fairly common, especially for custom made websites. This shows that running such a website is an ongoing process that requires long-term maintenance.

But, as CyberHUB-AM writes in its post-mortem blog post: "most Armenian companies see their websites as a refrigerator that you buy and put in the kitchen and forget about it for years." [11]

Thankfully, the organization was scheduled to have a new version of its website launched 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.

RATs

A Remote Access Trojan (RAT) is a form of malware that enables unauthorized remote access and control over a compromised computer system. RATs facilitate a range of malicious activities, including data exfiltration, surveillance, system manipulation, and leveraging the infected machine for further attacks. These Trojans are typically propagated through social engineering tactics, malicious attachments, or drive-by downloads, posing a significant threat to both individual users and organizational security.

In early 2023, two Armenian media outlets fell victim to sophisticated account takeover attacks targeting their Google/YouTube accounts. These incidents, occurring in January and March, were initiated through Remote Access Trojans (RATs) embedded in KMSauto software, a tool commonly used to illegally activate Microsoft Windows and Office products.

Once the RATs were deployed, the attackers gained control over the media outlets' accounts. They altered the YouTube account logos and names, repurposing them to promote Tesla cryptocurrency scams. This tactic not only disrupted the media outlets' operations but also aimed to deceive their audience into participating in fraudulent schemes.

The detailed analysis by Bitdefender[12] highlights the growing prevalence of such "stream-jacking" attacks, where legitimate YouTube channels are hijacked to broadcast scam content.

In a separate incident, starting from late 2022, Check Point Research identified a campaign targeting entities in Armenia. This campaign involved a new version of the OxtaRAT backdoor, an AutoIt-based tool designed for remote access and desktop surveillance. The malware was distributed via a self-extracting archive disguised as a PDF file, which deployed multiple files upon execution to compromise the target system.

The OxtaRAT backdoor is a tool capable of file exfiltration, video recording from webcams and desktops, remote control via TightVNC, and web shell installation. This version of OxtaRAT featured improved operational security and new functionalities compared to previous versions. The attackers targeted human rights organizations, dissidents, and independent media in Azerbaijan, marking the first known use of OxtaRAT against Armenian targets and corporate environments.

Researchers from Check Point collaborated with Cyberhub-AM's team[13] to uncover the full extent of this campaign. Their efforts revealed that the infection chain began with a file named "Israeli_NGO_thanks_Artsakh_bank_for_the_support_of.scr," submitted to VirusTotal from an IP address in Yerevan. This file executed commands to deploy the OxtaRAT malware using a lure PDF document related to Alexander Lapshin, a human rights activist.

The investigation highlighted the attackers' use of polyglot files, combining valid JPEG and AutoIt A3X formats, to evade detection. The OxtaRAT backdoor

contained approximately 20,000 lines of obfuscated AutoIt code, enabling various espionage activities. These included running additional code, installing PHP web shells, and performing reconnaissance on infected machines.

The Operation Silent Watch campaign underscores the ongoing cyber threats in the region. The collaboration between Check Point Research and Cyberhub-AM was instrumental in identifying and mitigating the impact of this malware. Their findings provide insights into the tactics, techniques, and procedures of the threat actors, enhancing the understanding of cyber espionage activities in conflict zones.

Insider attacks

Insider attacks are cybersecurity threats that originate from individuals within an organization who have authorized access to its networks or systems. These threats can be intentional, such as a disgruntled employee deliberately causing harm, or unintentional, resulting from negligence or human error. Insider attacks are particularly dangerous because they exploit legitimate access, making them harder to detect and prevent. They can lead to significant data breaches, financial losses, and damage to an organization's reputation.

In such an insider attack at an Armenian media company in April 2023, a disgruntled employee exploited remote access to the newsroom via TeamViewer to take control of the organization's YouTube channel. The employee, leveraging their legitimate access, managed to hijack the YouTube account, causing significant disruption. CyberHUB was instrumental in investigating the incident, meticulously tracing the attack's origin and identifying the methods used. They also coordinated with YouTube through AccessNow, successfully restoring the account to the TV company's control. This incident underscores the critical need for stringent internal security measures and vigilant monitoring of remote access protocols.

CONCLUSION

In a world where digital threats are becoming increasingly sophisticated and persistent, Armenia faces a complex and ever-evolving threat landscape. The ongoing conflict with Azerbaijan, coupled with the use of advanced spyware like Pegasus, has highlighted the country's vulnerability to state-sponsored cyberattacks. Phishing attacks, website hacks, and the deployment of Remote Access Trojans (RATs) have further exposed vulnerabilities in the digital infrastructure of media outlets, civil society organizations, and governmental institutions.

The incidents outlined in this report underscore the urgent need for Armenia to strengthen its cybersecurity frameworks and enhance its incident response capabilities. It is crucial for the country to collaborate internationally and invest in advanced threat detection and prevention measures to counter the growing threat of cyberattacks. Raising public awareness about cybersecurity risks and promoting safe online practices are equally important steps in building a more resilient digital ecosystem.

Key findings reveal that both external and internal actors are exploiting vulnerabilities in Armenia's systems, targeting civil society, media outlets, and governmental institutions. These threats not only endanger critical infrastructures but also erode trust in digital platforms and threaten human rights. The adaptive and collaborative measures taken by organizations like CyberHUB-AM, alongside international partnerships, are critical in mitigating these risks and bolstering the nation's cyber resilience.

As Armenia continues to navigate this challenging landscape, it is imperative for the government, private sector, and civil society to work together in building a more secure and resilient digital future.

SOURCES

1 "Freedom in the World 2023: Armenia." Freedom House. Accessed July 2023.

2 "Freedom in the World 2023: Armenia." Freedom House.

3 "Armenia police warn of growing cybercrime rate." Armenpress. Last modified June 12, 2018.

4 "Armenian police bust Yerevan-based cybercrime syndicate targeting U.S. users via tech support scam." Armenpress. Last modified May 1, 2019.

5 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.

6 Stone, Maddie and Clement Lecigne. "How we protect users from 0-day attacks." Google, Threat Analysis Group. July 14, 2021.

7 Nimmo, Ben, David Agranovich, and Nathaniel Gleicher. "Quarterly Adversarial Threat Report." Meta. April 2022.

8 "Armenia/Azerbaijan: Pegasus spyware targeted Armenian public figures amid conflict." Amnesty International. Published May 25, 2023. Accessed December 26, 2024.

9 Muhammad, Rafie. "Critical Privilege Escalation in Essential Addons for Elementor Plugin Affecting 1+ Million Sites." Patchstack. Last modified May 11, 2023.

10 Martin, Ben. "Vulnerability in Essential Addons for Elementor Leads to Mass Infection." SucriBlog. Last modified May 18, 2023.

SOURCES

11 "Hackers leverage vulnerability of Essential Addons plugin to exploit Armenian WordPress sites." CyberHUB. Last modified May 23, 2023.

12 "Armenia Country Threat Landscape Report." by CyberHUB 2023.docx. Sharepoint.com. Published 2023. Accessed December 3, 2024.

13 CyberHUB-AM. "Check Point Research uncovers Azerbaijani cyber attack against Armenian targets." Published February 17, 2023. Accessed February 7, 2025.