2025

ARMENIA CYBERSECURITY THREAT LANDSCAPE

Annual Report by CyberHUB-AM

Yerevan, 2025

Media Diversity Institute

CyberHUB-AM

Table of Content

Executive Summary ---- 02

Introduction ---- 04

Strategic Context ---- 05

Threat Landscape Analysis ---- 07

Incident Case Studies ---- 10

Armenia's Defensive Posture ---- 23

Conclusions and Strategic Outlook ---- 26

Appendix A:
Consolidated Indicators of Compromise ---- 29

Appendix B: References ---- 30

01

Executive Summary

The year 2025 marks a definitive inflection point in Armenia's digital security environment. As the country accelerates its strategic pivot toward the European Union and the United States — decoupling from legacy Russian security architectures — its digital domain has become the primary theater for hybrid warfare, punitive signaling, and intelligence collection.

This report, produced by CyberHUB-AM, documents and analyzes the principal cyber threats observed in Armenia throughout 2025. The overarching theme is “hybrid siege”: a sustained, multi-vector campaign conducted by both state-aligned adversaries and criminal groups that exploits Armenia's geopolitical transition and the approaching 2026 parliamentary elections.

Key Findings:

- State-sponsored threat actors, particularly Russian APT groups such as APT28 (Fancy Bear) and the Mandiant-attributed cluster UNC5792, have intensified targeted operations against Armenian civil society, government institutions, and independent media. These campaigns increasingly exploit encrypted messaging platforms — Signal, WhatsApp, and Telegram — rather than traditional email vectors.
- Mercenary spyware activity has shifted significantly: Pegasus infections, extensively documented in Armenia between 2020 and 2023 and attributed to Azerbaijani operators, dropped to zero in 2025, suggesting a potential transition to alternative surveillance tooling.
- Financial cybercrime targeting the Armenian banking sector has grown substantially, driven by Android banking trojans and fraudulent applications designed to exploit the rapid digitization of the economy and low population-level cyber hygiene.
- Civil society and independent media remain the most heavily targeted sectors, with at least eight significant incidents documented in 2025, including spearphishing campaigns impersonating EU ambassadors, government ministers, and National Security Service officers.
- Armenia has responded with landmark legislative and institutional reforms, including the adoption of the 2025 Law “On Cybersecurity” (effective 2026), the operationalization of AM-CERT under ISAA, and expanded public education initiatives including the CyberChat child safety platform.

Looking ahead, the intensity of foreign interference operations is expected to increase as the 2026 elections approach. Technical defenses alone are insufficient against adversaries who adapt in real time and exploit the human layer of security. A unified national response — combining critical infrastructure protection, specialized civil society defense, and digital literacy at scale — is essential.

02 Introduction

Purpose and Scope

The Armenia Cybersecurity Threat Landscape 2025 report provides a comprehensive analysis of the cyber threat environment affecting Armenia across the calendar year 2025. The report is produced by CyberHUB-AM, which serves as the de facto Computer Emergency Response Team (CERT) for Armenia's civil society and independent media sectors.

The report is intended to serve multiple audiences: policymakers and government officials seeking a strategic overview; security practitioners requiring technical indicators and attack pattern analysis; civil society organizations and media outlets that are primary targets of documented campaigns; and international partners and donors engaged in supporting Armenia's democratic and digital development.

The analysis is based on incident data collected and processed by CyberHUB-AM during 2025, supplemented by open-source intelligence, threat intelligence from partner organizations including Mandiant, Google Threat Intelligence, and Volexity, and public reporting from ISAA and the Armenian government. Case studies presented in Section 5 are drawn from incidents directly handled by or reported to CyberHUB-AM. Indicators of Compromise (IOCs) are presented in defanged format throughout the report.

03 Strategic Context

3.1 Armenia's Geopolitical Pivot

Armenia's cybersecurity environment in 2025 cannot be understood in isolation from its broader geopolitical transformation. The country is navigating a decisive strategic pivot — seeking closer integration with the European Union and the United States while managing the friction of decoupling from traditional Russian-led security architectures, including the Collective Security Treaty Organization (CSTO). This realignment, accelerated by Russia's failure to support Armenia during the 2023 Azerbaijani offensive in Nagorno-Karabakh, has made Armenia's digital domain the primary theater for punitive signaling and hybrid pressure.

Three structural factors make 2025 a particularly high-risk year. First, the formal deepening of EU-Armenia relations — including the progress of the EU-Armenia Partnership Agreement — provides foreign adversaries with strong motivation to undermine and surveil participants in the integration process, particularly civil society organizations and government officials. Second, the 2026 parliamentary elections represent a high-value target for foreign interference operations aimed at shaping Armenian political outcomes and discrediting democratic institutions. Third, Armenia's rapid digitization of the economy and public services, while positive for development, has outpaced the growth of population-level cyber awareness and organizational security maturity.

3.2 The Hybrid Siege Framework

The overarching theme of the 2025 threat landscape is what CyberHUB-AM characterizes as a “hybrid siege.” Unlike the kinetic conflicts of 2020 and 2023, where cyber operations served as tactical support for military maneuvers, the current aggression is strategic, persistent, and non-kinetic. The absence of active military hostilities on the border has not produced digital peace; rather, it has sublimated conflict into the cyber domain, where it can be conducted with greater deniability, lower costs, and sustained over time.

This hybrid siege operates simultaneously on two fronts. On the state-sponsored flank, sophisticated APT groups aligned with Russian and potentially other foreign intelligence services conduct targeted surveillance, credential theft, and influence operations against those capable of affecting Armenia's democratic and geopolitical trajectory. On the criminal flank, organized cybercrime groups — some of which may have tacit state tolerance — exploit Armenia's expanding digital economy and the financial inexperience of newly digital consumers.

3.3 Threat Actor Landscape

The principal threat actor categories active against Armenian targets in 2025 are:

- **Russian State-Aligned APT Groups:** APT28 (Fancy Bear), attributed to Russia's GRU military intelligence, has been observed targeting government infrastructure as a signaling mechanism. UNC5792, a cluster attributed by Mandiant with high confidence and corroborated by Google Threat Intelligence, conducted sustained spearphishing campaigns against civil society and electoral institutions via Signal.
- **Azerbaijani Intelligence Operations:** Previously the primary operator of Pegasus spyware against Armenian targets from 2020 to 2023, Azerbaijani services appear to have paused or replaced this capability in 2025. Zero Pegasus infections were detected during the reporting period, suggesting either a supplier change or a shift to less detectable collection methods.
- **International Cybercrime:** Criminal groups — likely operating from Eastern Europe and Central Asia — are targeting Armenian financial sector users with Android banking trojans including the Ajina.Banker family. These groups exploit the rapid digitization of payments and inadequate mobile security practices.
- **Unattributed Social Engineering Operators:** A sophisticated multi-stage fraud operation targeting Armenian journalists and civil society via WhatsApp and Viber, involving impersonation of peers and fake National Security Service officers, bears hallmarks of state-backed operational resources but has not been formally attributed.

04 Threat Landscape Analysis

4.1 State-Sponsored Operations and Spyware

State-sponsored cyber operations against Armenia in 2025 are characterized by a shift from blunt-force intrusion tactics toward highly targeted social engineering campaigns. The preferred attack surface has moved from government network perimeters to the personal devices and accounts of high-value individuals — civil society leaders, journalists, government officials, and electoral commission staff.

The most significant development in the spyware domain is the complete disappearance of confirmed Pegasus infections, which had been extensively documented against Armenian targets between 2020 and 2023. This cessation is unlikely to reflect a reduction in adversary interest; rather, it suggests a capability shift. Possible explanations include: transition to a new commercial spyware vendor not yet identified by current detection methods; increased use of zero-click exploits that leave fewer forensic traces; or a strategic shift toward social engineering-based access, which is cheaper and harder to attribute.

Concurrently, APT28 (Fancy Bear) activity directed at Armenian government infrastructure has been documented, consistent with patterns observed across post-Soviet states that have pursued Western alignment. These operations appear designed less for immediate data exfiltration and more for strategic signaling — demonstrating the capability to penetrate critical systems as a coercive tool.

4.2 Spearphishing and Social Engineering

Spearphishing — targeted phishing attacks using personalized lures against specific high-value individuals — is the dominant attack technique observed in 2025. A critical tactical evolution has occurred: threat actors have largely migrated from email-based delivery to encrypted messaging platforms, particularly Signal. This shift serves multiple attacker objectives: Signal's end-to-end encryption limits network-level detection; the platform carries a strong association with security and trustworthiness, making recipients less suspicious; and the conversational format enables real-time social engineering that email cannot replicate.

Eight documented incidents collectively reveal a consistent playbook: attackers conduct reconnaissance on targets' professional networks and institutional affiliations, construct credible impersonation personas (EU ambassadors, ministry officials, peer journalists), initiate contact via Signal or WhatsApp, and use the established false trust to deliver malicious links or extract authentication credentials. Several incidents demonstrate real-time attacker adaptability — when initial infrastructure is detected or expires, replacement URLs are provided within minutes, confirming active human operators rather than automated systems.

A particularly dangerous variant involves Microsoft 365 OAuth token theft. Rather than phishing for passwords, attackers guide victims through a legitimate Microsoft login flow, then instruct them to paste the resulting authentication token back to the attacker via Signal. This technique bypasses multi-factor authentication and allows attackers to enroll attacker-controlled devices into the victim's Microsoft Entra ID, granting persistent, legitimate-looking access to organizational resources.

4.3 Financial Cybercrime and Malware

The Armenian financial sector and its consumers face growing pressure from Android-targeting malware campaigns. The Ajina.Banker family, distributed through Telegram channels posing as legitimate banking or government service applications, is capable of intercepting SMS one-time passwords, harvesting banking credentials, and exfiltrating contact data. The malware exploits the same rapid digitization of financial services that has been a driver of Armenia's economic development agenda.

A documented 2025 case involved the distribution of ArmScan.apk — a malicious Android application hosted on the domain gov-am.sbs, designed to impersonate a government-backed cashback application. The social engineering premise — claiming users could scan receipts for government subsidies — was carefully designed to exploit public expectations around state support programs. The application was classified as a Trojan/Dropper, meaning it served both as an immediate data collection tool and a delivery mechanism for further malicious payloads.

These campaigns reflect a deliberate targeting strategy: Armenia's banking sector has been assessed as “a lucrative target” by criminal groups due to the explosion of digital payment adoption, the relative immaturity of consumer-level security awareness, and gaps in mobile threat detection infrastructure across financial institutions.

4.4 DDoS and Website Defacement

Distributed Denial of Service (DDoS) attacks and website defacements, while representing a less sophisticated attack category, continue to serve as tools of political signaling and disruption. These attacks typically spike around periods of heightened geopolitical tension and are used to demonstrate offensive capability, degrade public trust in digital services, and generate media coverage that amplifies the psychological impact of adversary operations.

In the 2025 context, DDoS attacks are best understood as part of the broader hybrid siege framework — low-cost, high-visibility actions that accompany more sophisticated and targeted operations rather than serving as standalone campaigns. Armenian government and media websites have been targets of defacement operations attributed to politically motivated actor groups with suspected state links.

4.5 Information Operations and Disinformation

Disinformation and influence operations targeting Armenian audiences have intensified alongside the acceleration of the country's EU integration process and the approach of the 2026 elections. These operations run across social media platforms, Telegram channels, and a network of websites producing content designed to undermine public confidence in the government's Western orientation, amplify political divisions, and discredit civil society organizations that advocate for democratic reforms.

The technical and social engineering incidents documented in this report have a dual function: beyond their primary purpose of credential theft or device compromise, they are also intelligence-gathering operations. The data harvested from compromised NGO accounts, journalists' communications, and civil society leaders' devices feeds directly into the targeting and refinement of subsequent influence operations.

A key observation from 2025 is the deliberate targeting of the trust infrastructure of Armenian civic life: by impersonating EU diplomats, ministry officials, and respected peer journalists, adversaries seek not only to compromise individual targets but also to erode the social trust that enables civic coordination and independent media to function effectively.

05 Incident Case Studies

The following case studies document eight significant cybersecurity incidents affecting Armenian civil society, media, and public sector organizations in 2025. Cases are organized thematically by attack type. All Indicators of Compromise (IOCs) are presented in defanged format.

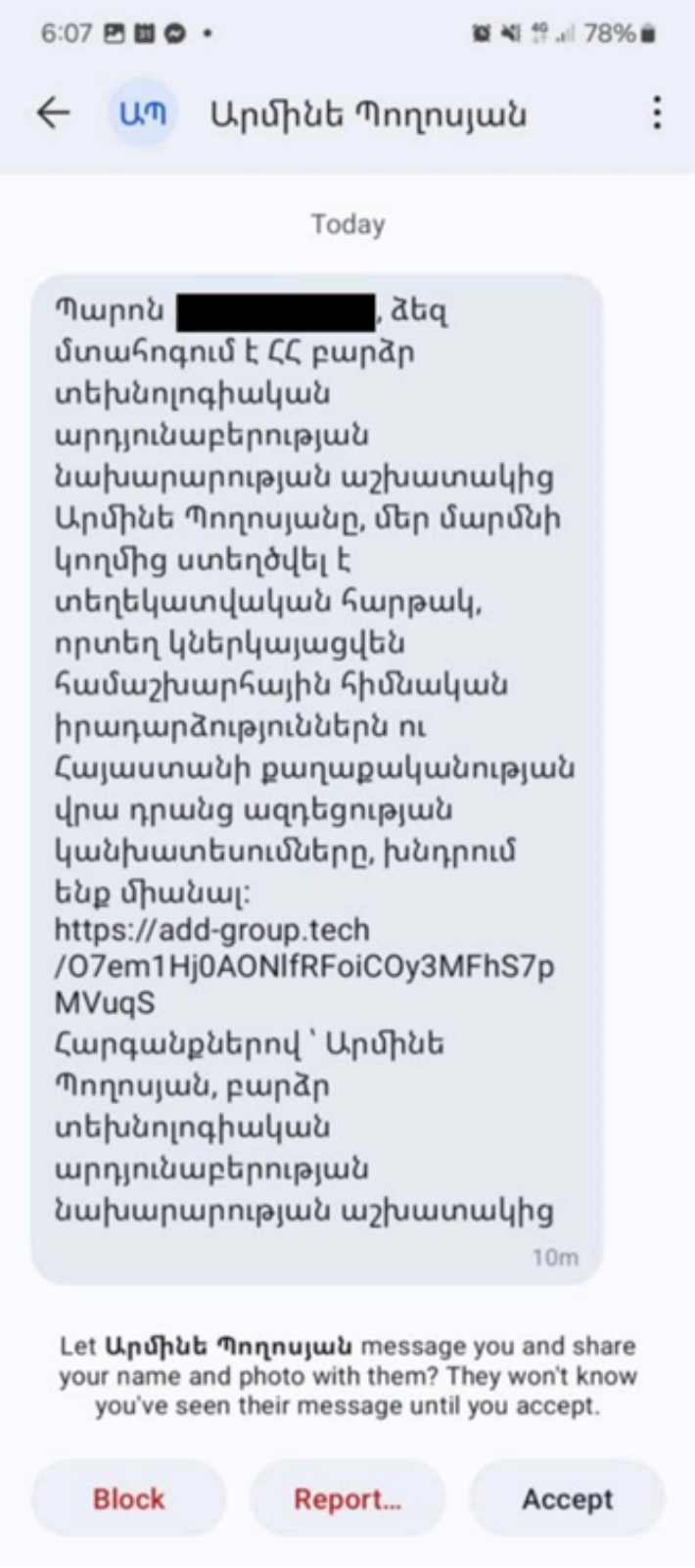
5.1 Spearphishing via Encrypted Messaging Platforms

Case 5.1.1: UNC5792 Signal Campaign — Ministry Impersonation

March–April 2025 | Target: Civil Society Organizations, Electoral Commission

In early March 2025, CyberHUB-AM identified a sustained spearphishing campaign targeting individuals and organizations within Armenia's civil society and public sector. The campaign has been attributed to UNC5792, an Advanced Persistent Threat cluster previously identified by Mandiant and corroborated by Google Threat Intelligence.

The attackers impersonated a fictional employee of Armenia's Ministry of High-Tech Industry named “Armineh Poghosyan,” using Signal to invite targets to join a purported “information platform” providing geopolitical analysis — a lure specifically calibrated to the professional interests of civil society analysts and NGO workers.



Screenshot of the UNC5792 phishing message sent via Signal, March 2025

Target Profile

- NGO active in legislative reform and election monitoring
- Security analyst involved in national-level policy and political analysis
- Armenian Electoral Commission staff

Key Tactics

- Attack delivered exclusively via Signal, bypassing email security controls
- Infrastructure was temporary: initial domain add-group.tech was replaced by group-add.com after detection
- Real-time operator engagement: when the first URL expired, a replacement was provided within minutes
- Three domains used: add-group.tech, group-add.com, signal-groups-add.com — all classified as high severity by VirusTotal

Indicator Type	Value	Description
Domain	add-group[.]tech	Initial delivery domain
Domain	group-add[.]com	Replacement domain after detection
Domain	signal-groups-add[.]com	Third-stage domain
URL	hxxps[://]add-group[.]tech/O7em1Hj0AONIfRFoIC0y3MFhS7pMVUqS	Initial phishing URL
URL	hxxps[://]group-add[.]com/kPDOT4Wr7PrKmkQtK6LrhFxmmo6LA7EE	Replacement phishing URL

Case 5.1.2: EU Ambassador Impersonation via Signal

April 8, 2025 | Target: Civil Society Organizations (dozens of NGOs)

A sophisticated spearphishing campaign targeting dozens of Armenian NGOs was identified on April 8, 2025. Attackers impersonated Vassilis Maragos, the EU Ambassador and Head of Delegation in Armenia, initiating contact via Signal messenger. The EU Delegation to Armenia was immediately notified and confirmed no compromise of its systems.

The phishing message invited recipients to a video conference titled “EU-Armenia Cooperation: Opportunities and Challenges for Civil Society,” scheduled via a link that appeared to be a legitimate Microsoft Teams meeting URL. The attack used a novel credential theft technique.

Attack Technique: Microsoft Entra ID Device Enrollment

Rather than directing victims to a fake login page, attackers directed targets to a legitimate Microsoft login portal. Upon successful authentication, the victim's browser generated a Microsoft authentication token. The attacker, communicating via Signal, then instructed the victim to copy and paste this token back — triggering a Microsoft Entra ID device joining process that enrolled an attacker-controlled device into the victim's account.

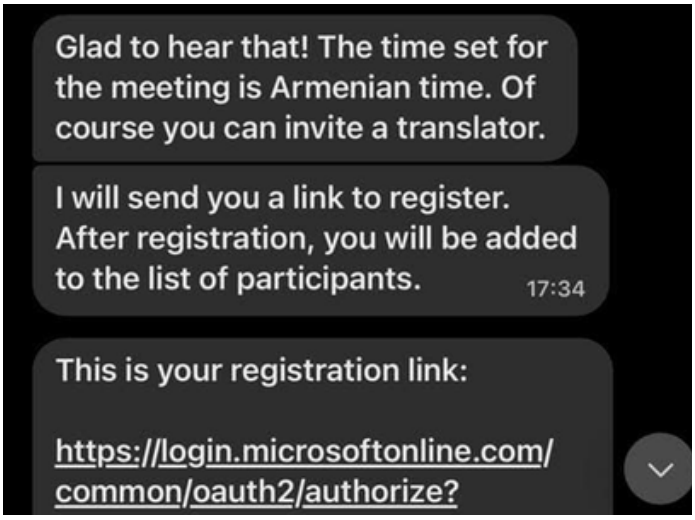
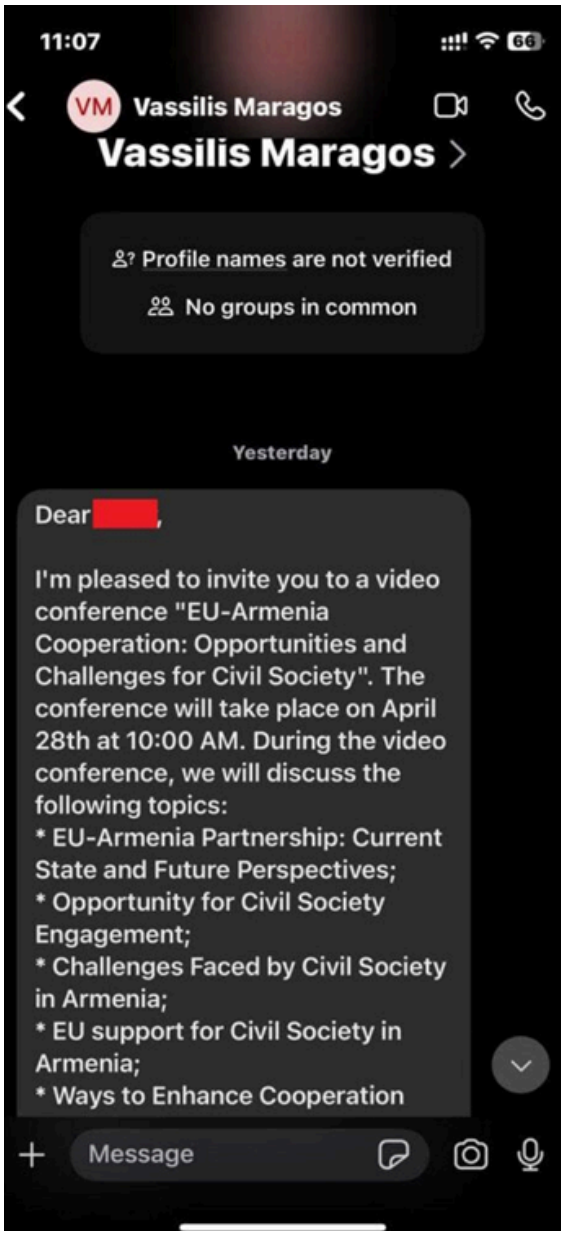


Illustration of the Entra ID device enrollment attack flow



Screenshot of the phishing message impersonating the EU Ambassador, April 2025

CyberHUB-AM confirmed the successful compromise of at least one Civil Society Organization leader's account. Forensic analysis revealed authentication attempts from three IP addresses, all attributable to Biterika Group LLC, a Russian cloud infrastructure provider.

Microsoft Authentica...	Failure	50053	95.182.124.124	Zelenograd, Moskva,...
Microsoft Azure CLI	Failure	50053	2605:6400:8583:2bef...	New York, New York,...
Microsoft Authentica...	Failure	50053	46.8.213.90	Zelenograd, Moskva,...

Log entries showing Microsoft Azure CLI login attempts from attacker-controlled Russian infrastructure

When the initial compromise was disrupted by incident response, attackers re-engaged the victim via Signal and attempted to repeat the procedure, claiming a technical error. This persistence is consistent with UNC5792 TTPs and with Russian threat actor behavior documented in Volexity's April 2025 report “Phishing for Codes: Russian Threat Actors Target Microsoft 365 OAuth Workflows.”

Indicator Type	Value	Description
IP Address	95[.]182[.]124[.]124	Attacker infrastructure — Biterika Group LLC (Russia)
IP Address	46[.]8[.]213[.]90	Attacker infrastructure — Biterika Group LLC (Russia)
IP Address	188[.]130[.]142[.]95	Attacker infrastructure — Biterika Group LLC (Russia)

Case 5.1.3: Signal Account Takeover Campaign

September 23, 2025 | Target: General Signal users in Armenia

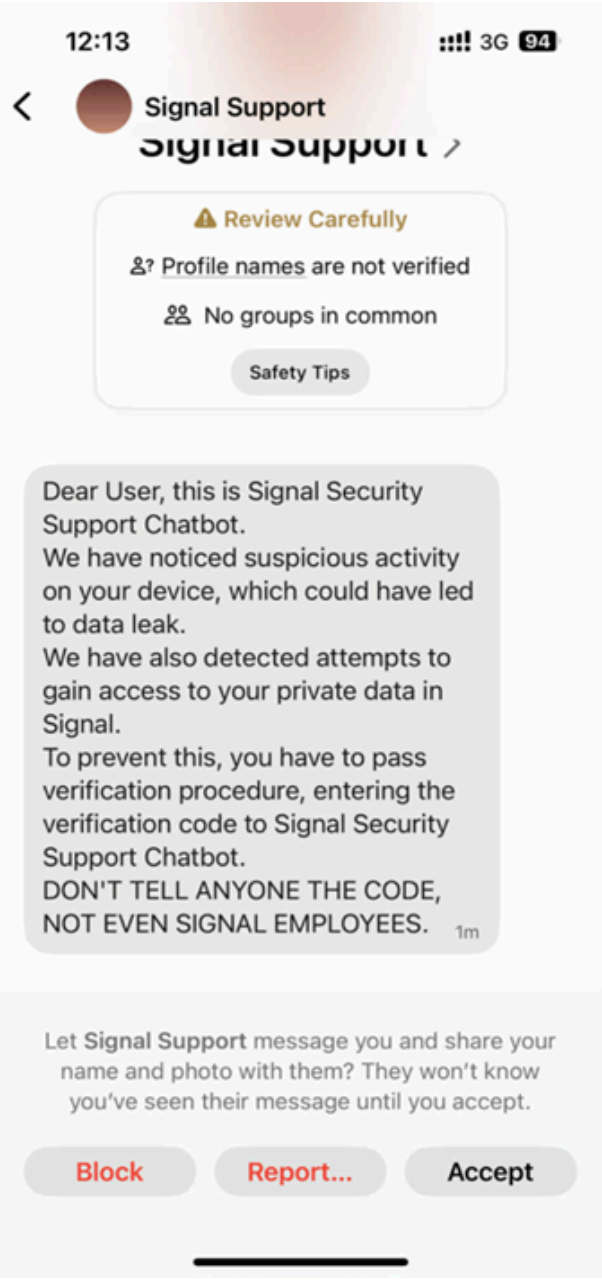
A threat actor conducted a phishing campaign on Signal aimed at hijacking user accounts by impersonating “Signal Support.” The attack exploited social trust in the Signal brand and targeted users who had not enabled the platform's Registration Lock feature.

Attack Sequence

1. Target receives an unsolicited Signal message from a contact named “Signal Support” claiming to have detected suspicious activity on the account.
2. The threat actor simultaneously initiates a real Signal registration request for the victim's phone number on an attacker-controlled device, causing Signal's backend to send a legitimate 6-digit OTP to the victim.
3. The attacker instructs the victim to provide the OTP “to verify their identity.”
4. If the victim complies and Registration Lock is not enabled, the attacker successfully re-registers the account to their device.

Critical Defense

This attack is completely neutralized by enabling Signal's Registration Lock feature (Signal Settings > Account > Registration Lock). When enabled, a user-created PIN is required to re-register a phone number, rendering the OTP alone insufficient for account takeover.



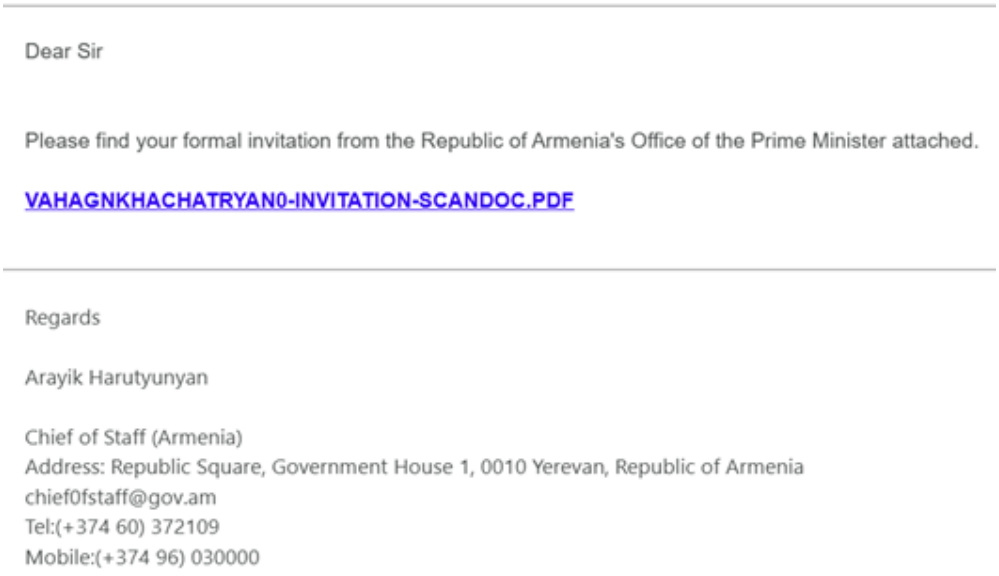
Screenshot of the Signal Support impersonation message

5.2 Email and Multi-Platform Phishing

Case 5.2.1: Targeted Phishing Against Armenian NGO via Prime Minister Impersonation

May 28–29, 2025 | Target: Armenian NGO (CyberHUB-AM partner)

On May 28, 2025, CyberHUB-AM identified a sophisticated phishing attack against one of its NGO partners. The attacker sent a phishing email containing a PDF attachment link, disguised as an official invitation from the Prime Minister's Chief of Staff (using the name VAHAGN KHACHATRYAN in the filename), indicating prior target reconnaissance.



Dear Sir

Please find your formal invitation from the Republic of Armenia's Office of the Prime Minister attached.

VAHAGNKHACHATRYAN0-INVITATION-SCANDOC.PDF

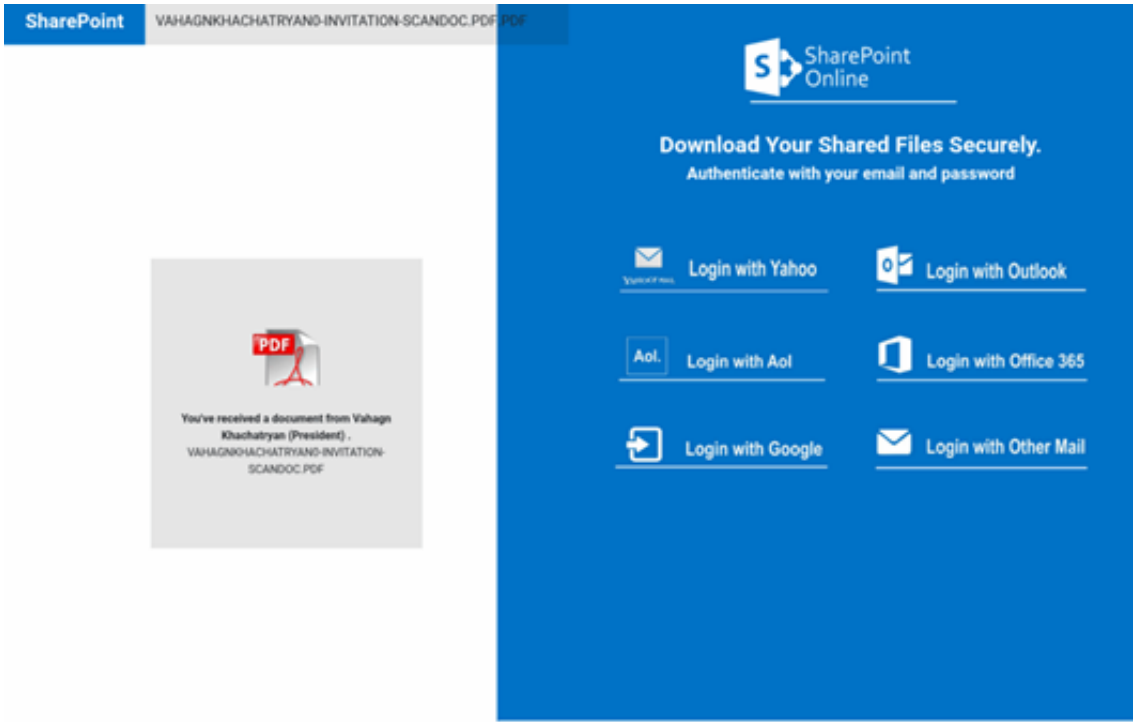
Regards

Arayik Harutyunyan

Chief of Staff (Armenia)
Address: Republic Square, Government House 1, 0010 Yerevan, Republic of Armenia
chief0fstaff@gov.am
Tel:(+374 60) 372109
Mobile:(+374 96) 030000

Screenshot of phishing email sent on behalf of the Prime Minister's Chief of Staff, May 2025

The redirect chain used the URL shortener Snip.ly to mask a GitHub Pages site (asw910.github.io) crafted to mimic official content. Embedded JavaScript masquerading as jquery.min.js performed credential harvesting and exfiltrated captured credentials via HTTP POST to a compromised WordPress site.



Screenshot of the credential harvesting phishing page targeting the NGO

MITRE ATT&CK Mapping

- T1566.001 — Spearphishing Attachment
- T1584 — Compromise Infrastructure (GitHub Pages, WordPress)
- T1204.002 — User Execution: Malicious File
- T1056.001 — Input Capture via credential form
- T1071.001 — Application Layer Protocol: Web

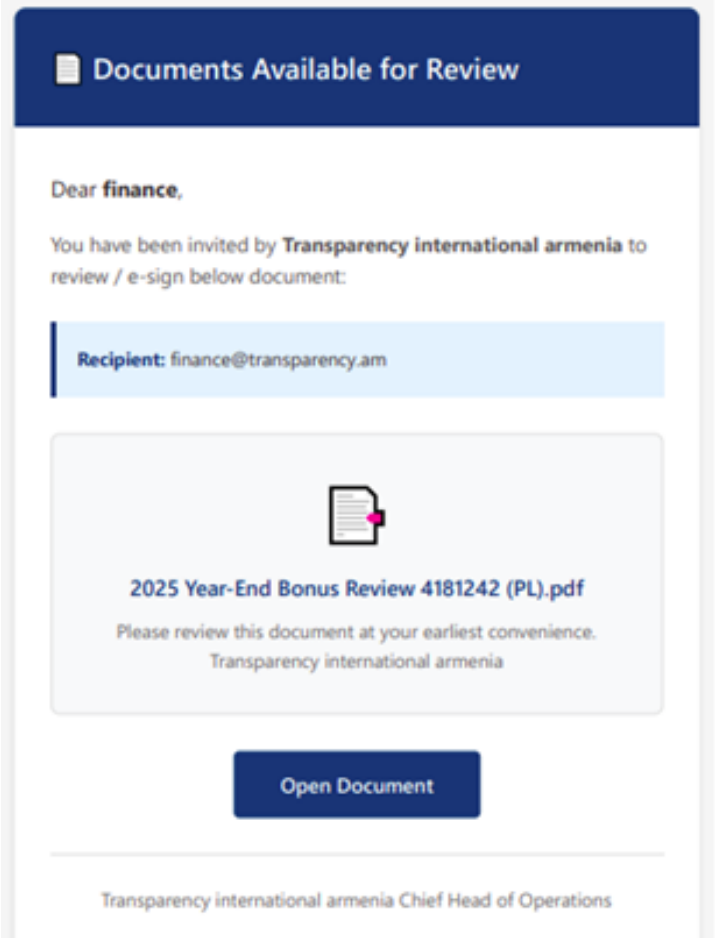
Indicator Type	Value	Description
URL	hxxps[://]snip[.]ly/l9xqzf	Initial redirect URL
Domain	asw910[.]github[.]io	GitHub Pages payload host
URL	hxxps[://]wbbuffetchurrascobh[.]com[.]br/wp-admin/email[.]php	Credential exfiltration endpoint

Case 5.2.2: PDF → Google Maps → AWS Phishing Chain

December 18, 2025 | Target: Transparency International Armenia

Transparency International Armenia was targeted by a phishing campaign using a multi-stage redirect chain designed to evade link-scanning tools. The attack began with emails bearing the subject line "Documents Pending your review," sent from the domain medinex[.]in (an Indian medical supply company with no connection to the target), using a fake reference ID to appear official.

The email contained a PDF attachment featuring a large, centrally placed "Open Document" button. On mouseover, the link appeared to point to Google Spain (maps.google.es), but on click redirected to a malicious AWS S3 bucket. This use of a trusted Google URL as a masking layer is specifically designed to bypass email security tools and deceive recipients who hover over links before clicking.



Screenshot of the malicious PDF document with the embedded redirect button, February 2026

Red Flags

- Generic greeting ("Dear finance") combined with urgency language
- PDF is a single image with a button — no legitimate document requires this format
- Sender domain (medinex.in — medical supply, India) has no logical connection to the content
- Visible URL differs from actual redirect destination

Indicator Type	Value	Description
Domain	medinex[.]in	Sender domain — Indian medical supplier
URL	hxxps[://]maps[.]google[.]es/url?q=[redirect]	Google Maps masking URL
URL	hxxps[://]bombapratclfnbjsmlkd58493849indexhtml[.]s3-website-us-east-1[.]amazonaws[.]com	Actual malicious destination (AWS S3)

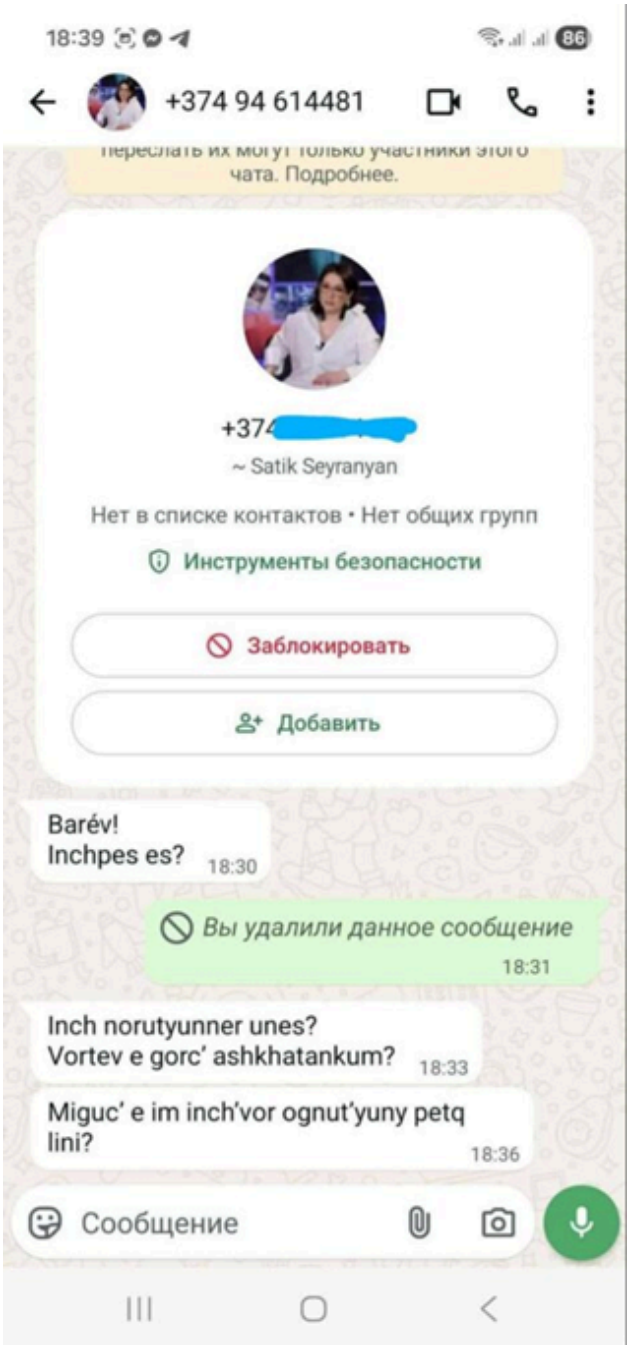
5.3 Social Engineering and Financial Fraud

Case 5.3.1: Multi-Stage WhatsApp Scam — NSS Impersonation

October–November 2025
Target: Armenian journalists and civil society representatives

In late October 2025, a highly sophisticated multi-stage social engineering operation targeted representatives of Armenian media and civil society. The operation is notable for its investment of human resources, its use of AI-assisted translation, and its potential dual purpose: financial fraud and intelligence collection or coercion.

The attack exploited hacked Armenian phone numbers to create fake WhatsApp accounts impersonating well-known colleagues of the target. The editor of Armenian outlet "168 Zham" publicly reported that her identity had been used in fake accounts targeting other journalists.



Screenshot of a WhatsApp account impersonating the editor of Armenian outlet 168 Zham

Attack Sequence

1. An attacker impersonating a known professional contacts the target on WhatsApp, claiming to have a new number.
2. After establishing rapport with personalized conversation (enabled by research into the target's professional network), the impersonator claims they have been falsely implicated in financial crimes involving Azerbaijani criminal proceeds.
3. The impersonator states that Armenia's National Security Service (NSS) is investigating and requests the target's cooperation.
4. A second actor calls the target, posing as an NSS officer, speaking in Russian and claiming a joint Armenia-Azerbaijan law enforcement operation.
5. The fake NSS officer instructs the target to transfer their personal funds to a “secure NSS account” to separate them from the alleged criminal proceeds.

Screenshot showing suspected AI translation error — one word left untranslated in Russian, revealing non-native operator

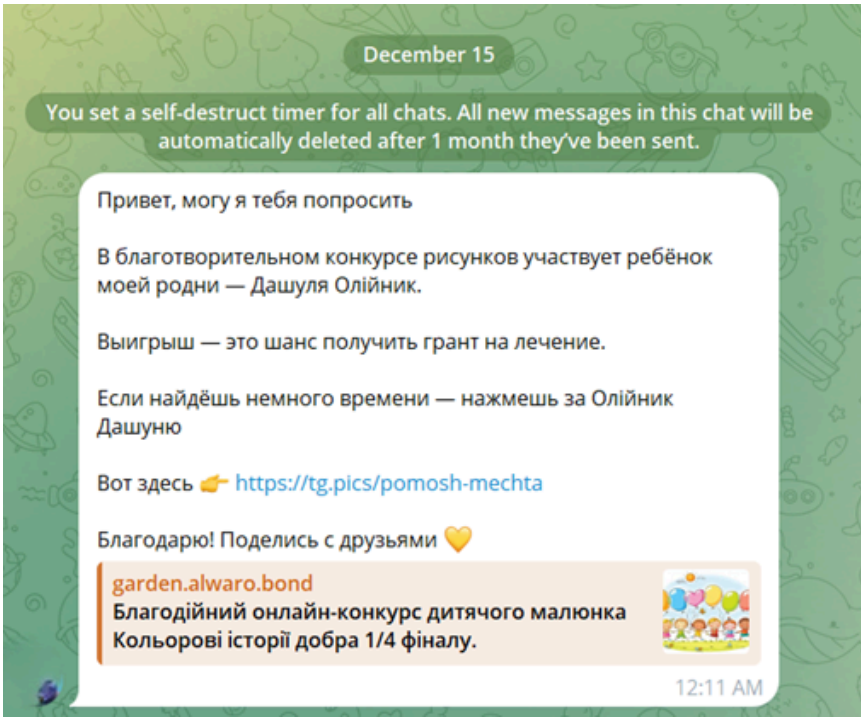
All targeted individuals identified the fraud before funds were transferred, either independently or after being alerted by CyberHUB-AM.

CyberHUB-AM's assessment is that beyond financial theft, the operation may aim to gather intelligence or create leverage for future coercion of high-profile civil society and media figures. The level of pre-operation research and human resource investment is consistent with the Russian-nexus threat actor COLDRIVER (also known as Star Blizzard, UNC4057, or Callisto). The campaign's use of WhatsApp and the impersonation of professional colleagues mirrors the group's documented strategic pivot toward mobile messaging platforms and persistent "long game" rapport-building designed to bypass institutional security.

Case 5.3.2:
Telegram “Vote for My Relative” Account Takeover Campaign

December 2025 | Target: General Telegram users in Armenia

One of the most widespread social engineering attacks observed in December 2025 exploits emotional manipulation and trust in known contacts. The attack begins with a message — sent from a compromised Telegram account belonging to someone the victim knows — asking for help voting for “a child in a charity contest.”



Screenshot of the initial “vote for my relative” solicitation message, December 2025

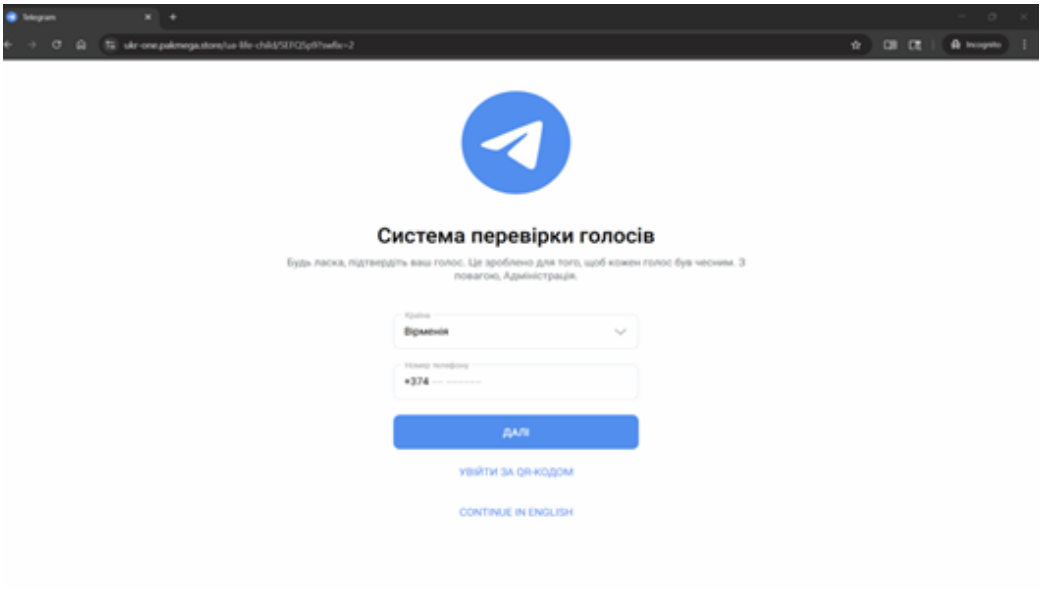
Attack Mechanics

- The message contains a link that appears to be Telegram-related (e.g. tg[.]pics/pomosh-mechta) but redirects via multiple chains to a fraudulent voting page.
- The fraudulent page is professionally designed, featuring children's artwork, countdown timers, and sponsor logos to maximize credibility.
- The site exhibits adaptive evasion: when accessed by automated analysis tools (VirusTotal, URLScan), it redirects to innocuous content (e.g. TikTok). When accessed from a genuine mobile browser, it presents the attack.
- Clicking “Vote” leads to a “verification” page that requests the victim's phone number, then silently initiates a real Telegram login request in the background, causing Telegram to send a legitimate login OTP to the victim's device.
- The page instructs the victim to enter the received code “to verify,” granting the attacker full account access.

Screenshot of the professionally designed fake charity contest page

Prevention

- Never enter a Telegram login code on any website — these codes are only for use inside the Telegram app itself
- Enable Two-Step Verification in Telegram settings
- If you receive such a message, contact the sender via another channel to verify — their Telegram account is likely compromised



Screenshot of the "vote verification" page initiating live Telegram account hijacking

5.4 Malware and Fraudulent Applications

Case 5.4.1: ArmScan.apk — Fake Government Cashback App

December 16, 2025 | Target: Armenian smartphone users

A malicious Android application named ArmScan.apk was distributed via the domain gov-am.sbs, impersonating a government-backed financial tool. The landing page claimed users could scan purchase invoices and receive government cashback payments — a premise designed to exploit public trust in state subsidy programs. The domain's WHOIS registration shows a connection to Malaysia, with no legitimate government affiliation.

VirusTotal classified the application as malicious (low severity on initial detection). Multiple antivirus engines subsequently identified it as a Trojan/Dropper — meaning it is capable of both exfiltrating data from the device and downloading additional malicious modules, potentially including banking credential stealers.

User Protection Guidance

- Install applications only from the official Google Play Store
- Verify government service claims by checking official .gov.am domains
- Treat unsolicited cashback or subsidy app promotions with high suspicion
- Never enter banking credentials or personal ID numbers into apps distributed outside official channels
- Disable “Install from Unknown Sources” in Android settings

Indicator Type	Value	Description
Domain	gov-am[.]sbs	Malicious distribution site impersonating Armenian government
File	ArmScan[.]apk	Malicious Android application (Trojan/Dropper)
Hash (SHA256)	ece1d80a3d0d8fea0d635d6acf432f75d15355bcc8cab62a0089a6a72b909a90	ArmScan.apk

Armenia's Defensive Posture

06

In recognition of the accelerating threat environment, Armenia undertook a substantial overhaul of its cybersecurity governance framework in 2025. The response spans legislative reform, institutional development, civil society capacity building, and public education.

6.1 The Law on Cybersecurity

The adoption of the comprehensive Law “On Cybersecurity” in 2025 constitutes the cornerstone of Armenia's new defensive posture. Set for full enforcement in 2026, the legislation introduces critical regulatory mechanisms previously absent from the Armenian legal framework.

Key Provision	Description	Strategic Impact
Vital sectors	Defines sectors of key importance for the normal functioning of the population, economic activity, state security, public health and safety, environmental protection, and the safeguarding of other vital interests of the state.	Establishes the sectors within which cybersecurity requirements apply to information systems, including obligations related to cyber incident detection, notification, prevention, response, oversight, and cybersecurity auditing.
Critical Information Infrastructure (CII)	Defines legal criteria for identifying CII in sectors including energy, banking, and telecommunications.	Requires operators to implement cybersecurity requirements and undergo cybersecurity audits based on applicable international or national standards.
Incident Reporting	Establishes mandatory timelines for public and private entities to report breaches to the national CERT.	Improves national threat visibility and enables rapid cross-sectoral response.

Key Provision	Description	Strategic Impact
Standardization	Introduces cybersecurity governance and security requirements for information systems operating in vital sectors and critical information infrastructure. Provides for the development of a national cybersecurity standard, as well as the designation of applicable international standards for different sectors.	Establishes a unified national framework for cyber risk management, incident response, monitoring, and cybersecurity audits. Facilitates deeper cooperation with Western partners and improves the investment climate.
Regulatory Authority	Mandates the creation of an independent government agency with formal oversight and enforcement capabilities.	Centralizes governance, reducing fragmentation of responsibility across ministries.

6.2 Reforms in Personal Data Protection

In 2025, Armenia launched a reform to transform its personal data protection (PDP) supervisory body into a fully independent and better-resourced personal data protection authority (PDPA). While primarily a data protection initiative, it also strengthens cybersecurity, as Armenia's PDP Law applies across all sectors and establishes safeguards for personal data, including in areas not covered by the Cybersecurity Law.

The reform significantly enhances the PDPA's institutional capacity. The current authority has limited staff and resources, restricting its oversight of data processing across public and private sectors. Strengthening independence and capabilities will improve enforcement of key obligations, including mandatory disclosure of data breaches. The reform began in August 2025 through a one-year EU-funded project, with the main objective of preparing legislative amendments to ensure the PDPA's full independence.

Political support was confirmed on October 31, 2025, during a consultation chaired by the Prime Minister, which presented the concept for a new independent PDPA and reviewed implementation steps. On November 5, 2025, the European Commission handed over the Armenia–EU Visa Liberalization Action Plan, which includes benchmarks for personal data protection, including establishing an independent supervisory authority, implementing PDP legislation across sectors, and developing training and guidance for public institutions. These measures are expected to strengthen Armenia's governance framework and contribute to a more resilient digital and cybersecurity environment.

6.3 Institutional Development: ISAA and AM-CERT

The Information Systems Agency of Armenia (ISAA), founded in 2022 and substantially empowered by the 2025 legislation, soon to be reformed further into an independent government regulatory authority (Commission), serves as the operational hub of the country's cyber defense architecture. Key developments in 2025 include:

- **AM-CERT Operationalization:** The National Computer Emergency Response Team (AM-CERT), operating under ISAA supervision, participated in international cyber drills in October 2025 in collaboration with the International Telecommunication Union (ITU), testing national readiness to respond to simulated APT attacks on critical infrastructure.
- **Sectoral Defense:** The Central Bank of Armenia continues to maintain a mature sectoral CSIRT for the financial industry, providing specialized incident response for banking sector institutions.
- **Digital ID (YesEm):** ISAA is leading the YesEm digital identity project, providing a secure, unified authentication system for government services. Protecting this platform from compromise is a top priority, as it represents a single point of failure for multiple public services.

6.4 Civil Society: CyberHUB-AM's Role

CyberHUB-AM has consolidated its position as the de facto CERT for Armenia's civil society and independent media sectors. In 2025, CyberHUB-AM provided critical incident response for NGOs and activists, uncovering targeted spyware attacks and sophisticated spearphishing campaigns. The eight cases documented in Section 5 were identified, analyzed, or responded to by CyberHUB-AM team.

This civil society-facing security capacity plays a complementary and irreplaceable role alongside state institutions: adversaries deliberately target organizations that are politically sensitive, under-resourced, and outside the coverage of government cybersecurity bodies. CyberHUB-AM's ability to serve these organizations with technical expertise, rapid incident response, and targeted digital security training fills a structural gap in Armenia's overall defensive architecture.

6.5 Education and Public Awareness

- **Cyber Month" Campaign:** A nationwide awareness initiative launched by the Ministry of High-Tech Industry and ISAA, featuring workshops and seminars across Armenia throughout 2025.
- **School Digital Safety Program:** A partnership with UNICEF and educational NGOs to integrate digital safety curricula into public schools, directly targeting the human-layer vulnerabilities exploited by social engineering campaigns.
- **CyberChat Platform (chat.cyberhub.am):** Launched by CyberHUB-AM with support from UNICEF and the Embassy of the United Kingdom, this digital helpline provides children and adolescents with a mechanism to report cyberbullying and online threats. It represents Armenia's first dedicated online safety platform for youth.

07 Conclusions and Strategic Outlook

7.1 The Hybrid Siege Continues

The evidence documented in this report confirms that Armenia faces a sustained, multi-vector cyber campaign that is political in motivation, professional in execution, and growing in sophistication. The “hybrid siege” framework accurately characterizes the operating environment: conflict has migrated from kinetic theaters to the digital domain, where it is conducted with greater deniability, lower cost, and continuous rather than episodic intensity.

The shift from email to encrypted messaging platforms as the primary attack vector is the most important tactical evolution of 2025. It represents a deliberate adaptation to improved organizational email security and reflects a deeper strategic insight: that the most valuable targets — civil society leaders, journalists, government officials — use Signal and WhatsApp as their primary communications channels for sensitive professional work. Defenders must adapt accordingly.

7.2 The 2026 Election Risk Window

As Armenia's 2026 parliamentary elections approach, CyberHUB-AM assesses with high confidence that the frequency and intensity of foreign interference operations will increase. The documented 2025 campaigns represent a pre-positioning phase: establishing infrastructure, identifying high-value targets, testing social engineering approaches, and harvesting credentials and organizational access for use in subsequent operations.

Election-related threats will likely manifest across multiple dimensions simultaneously: technical attacks against electoral infrastructure and government communications; influence operations designed to amplify social divisions and undermine confidence in the integrity of the process; targeted harassment and compromise of candidates, party officials, and election monitors; and financial fraud operations designed to discredit civil society organizations engaged in election observation.

7.3 Recommendations by Stakeholder

For Government and Regulatory Bodies

- Accelerate implementation of the 2025 Law “On Cybersecurity,” particularly mandatory incident reporting requirements, ahead of the formal 2026 deadline.
- Establish a dedicated pre-election cybersecurity task force coordinating AM-CERT, law enforcement, and the Central Election Commission.
- Expand information-sharing mechanisms with EU cybersecurity institutions (ENISA) and allied national CERTs, leveraging Armenia's EU integration progress.
- Mandate Microsoft 365 security baseline configurations — including Entra ID Conditional Access and device enrollment policies — across government institutions.

For Civil Society Organizations and Independent Media

- Implement Signal Registration Lock and Telegram Two-Step Verification across all organizational accounts without exception.
- Establish internal verification protocols for any request — regardless of apparent source — to click links, provide credentials, or transfer funds.
- Contact CyberHUB-AM for organizational digital security assessments and targeted training, particularly ahead of the election period.
- Treat all unsolicited contact from officials, diplomats, or security service representatives via messaging platforms as potentially fraudulent until verified through independent channels.

For Businesses

- Organizations that fall under the scope of the Law “On Cybersecurity” - prepare for compliance with the Law, even if formal obligations will take effect later, allocate dedicated resources and funding to support cybersecurity measures.
- Even if not formally required, organizations outside the Law “On Cybersecurity” can benefit from voluntarily adopting relevant cybersecurity measures.
- All Businesses

- Use secure communication channels and enable two-factor authentication across all corporate accounts.
- Conduct periodic internal and third-party cybersecurity audits.
- Contact CyberHUB-AM for support such as digital security assessments, training, and guidance to strengthen organizational resilience.
- Etc...

For the General Public

- Never share OTPs or verification codes received via SMS with any third party, through any channel.
- Install applications only from official app stores; be deeply suspicious of apps promoting government subsidies, cashback, or financial benefits.
- Enable two-factor authentication on all banking and financial applications.
- Report suspected phishing or fraud attempts to CyberHUB-AM (cyberhub.am) and, for financial fraud, to the relevant bank's security team.

7.4 Closing Assessment

The security of Armenia's democratic institutions now depends on a unified approach that goes beyond technical controls. Adversaries have demonstrated they will adapt to defensive measures in real time, escalate from one compromised target to the next, and exploit the social and institutional trust that makes civic life function. Resilience against this threat requires not only stronger infrastructure and better technology, but also a population-wide culture of digital vigilance, and a sustained, well-resourced civil society security sector capable of defending those whom the state cannot reach.

CyberHUB-AM remains committed to providing this capability, and calls on government bodies, international partners, and the private sector to recognize and support the essential role that civil society cybersecurity plays in Armenia's democratic resilience.

Appendix A: Consolidated Indicators of Compromise

All IOCs documented in this report are presented below in consolidated form. All values are in defanged format.

Case	Type	Indicator	Notes
5.1.1 UNC5792	Domain	add-group[.]tech	Initial delivery domain
5.1.1 UNC5792	Domain	group-add[.]com	Replacement domain
5.1.1 UNC5792	Domain	signal-groups-add[.]com	Third-stage domain
5.1.2 EU Ambassador	IP	95[.]182[.]124[.]124	Biterika Group LLC (Russia)
5.1.2 EU Ambassador	IP	46[.]8[.]213[.]90	Biterika Group LLC (Russia)
5.1.2 EU Ambassador	IP	188[.]130[.]142[.]95	Biterika Group LLC (Russia)
5.2.1 Razer	Domain	razer-us[.]com	Fake domain (reg. Dec 12, 2024)
5.2.1 Razer	IP	198[.]54[.]127[.]77	Mail server
5.2.1 Razer	IP	198[.]54[.]118[.]220	Hosting server
5.2.1 Razer	SHA256	693cc086...736bce4	msimg32.dll
5.2.1 Razer	SHA256	08c7fb60...10f7a2	Malicious .exe
5.2.2 NGO Phish	Domain	snip[.]ly	URL shortener used
5.2.2 NGO Phish	Domain	asw910[.]github[.]io	GitHub Pages payload host
5.2.2 NGO Phish	URL	hxxps[://]wbbuffetchurrascobh[.]com[.]br/wp-admin/email[.]php	Credential exfiltration endpoint
5.2.3 TI Armenia	Domain	medinex[.]in	Sender domain
5.2.3 TI Armenia	Domain	amazonaws[.]com (S3)	Malicious final destination
5.4.1 ArmScan	Domain	gov-am[.]sbs	Fake gov distribution site
5.4.1 ArmScan	SHA256	ece1d80a3d0d8fea0d635d6acf432f75d15355bcc8cab62a0089a6a72b909a90	ArmScan.apk

Appendix B: References

- Armenia Cybersecurity Threat Landscape 2024 — CyberHUB-AM: https://cyberhub.am/en/blog/2025/06/26/armenia-cybersecurity-threat-landscape-2024-eng/
- Armenia Country Threat Landscape Report 2024 — MDI: https://mdi.am/wp-content/uploads/2025/06/Armenia__Threat_Landscape_2024_ENG.pdf
- Spear Phishing in Armenia: Inside a Persistent Campaign by UNC5792 — CyberHUB-AM: https://cyberhub.am/en/blog/2025/05/31/spear-phishing-in-armenia-inside-a-persistent-campaign-by-unc5792/
- Cybersecurity Threats Facing Armenia In 2026 — Media.am: https://media.am/en/critique/2025/12/19/44393/
- New Android Malware 'Ajina.Banker' — The Hacker News: https://thehackernews.com/2024/09/new-android-malware-ajinabanker-steals.html
- Building the Architecture of Cybersecurity: Armenia's Institutional Turn — EVN Report: https://evnreport.com/politics/building-the-architecture-of-cybersecurity-armenias-institutional-turn/
- Law on Cybersecurity (Armenian) — ARLIS: https://www.arlis.am/hy/acts/218672/latest
- International CyberDrill in Armenia — ISAA: https://isaa.am/en/articles/international-cyberdrill-in-armenia-strengthening-resilience
- Armenia's Digital ID Solution (YesEm) — ISAA: https://isaa.am/en/armenia%E2%80%99s-digital-id-solution
- Launch of Cyber Month 2025 in Armenia — ISAA: https://isaa.am/en/articles/launch-of-cyber-month-2025-in-armenia
- New Partnership to Advance Children's Online Safety in Armenia — UNICEF: https://www.unicef.org/armenia/en/press-releases/new-partnership-advance-childrens-online-safety-armenia
- Phishing for Codes: Russian Threat Actors Target Microsoft 365 OAuth Workflows — Volexity: https://www.volexity.com/blog/2025/04/22/phishing-for-codes-russian-threat-actors-target-microsoft-365-oauth-workflows/
- Multiple Russian Threat Actors Targeting Microsoft Device Code Authentication — Volexity: https://www.volexity.com/blog/2025/02/13/multiple-russian-threat-actors-targeting-microsoft-device-code-authentication/