Threat Report: NSS-Impersonation Lure Delivering a PowerShell Backdoor to the Armenian Diaspora (September 2026)

Reference: CHAM-IN-2026-09-28 | **Date:** 28 September 2026 | **Classification:** TLP:AMBER | **Status:** Initial analysis, single sample

> Scope: this note is based on static analysis of one lure file submitted to CyberHUB-AM, and on the samples recovered from it. No stage was executed; all behaviour described is read directly from recovered code and configuration. Command-and-control infrastructure was not contacted beyond passive reputation and registration lookups. Victim telemetry, delivery emails, and server-side tasking were not available.

1. Executive Summary

A PDF titled “Hovel Chernokian SNS CASE for Armenian Diaspora” impersonates the National Security Service of the Republic of Armenia (NSS) and instructs “dear colleagues” to click a button to view attached case files. The click triggers embedded Acrobat JavaScript that drops a RAR archive containing decoy CVs of real diaspora members, an identity-document image, and a Windows executable disguised as a PDF. Execution leads, through two nested WinRAR self-extracting archives, to an AES-encrypted and base64-layered PowerShell backdoor persisted via scheduled tasks.

- The final implant screenshots the victim’s screen every 10–20 seconds and polls a C2 server for commands: arbitrary shell execution, targeted and mass file exfiltration, archive staging, file download, internal port scanning, and reverse SSH tunnelling into the victim’s network.
- C2: conference[.]sources-debian[.]info (tasks.php / upload.php / tools/). No public threat-intelligence reporting on this domain was found as of 28 September 2026.
- Targeting is aimed at the Armenian diaspora and people who work with it, using state-authority branding and personal documents of real individuals (ASSESSMENT).
- Attribution is not established. The tradecraft is consistent with a targeted espionage operation rather than financially motivated crimeware (ASSESSMENT).

2. Lure Document

DOCUMENTED. The PDF (8.4 MB, PDF 1.7, one page) is encrypted with AES-256 and an empty user password, and its metadata was stripped with ExifTool. The visible text, in Armenian, reads in translation: “Dear colleagues, to review the information in the attached PDF file, double-click the button below to view the attachments. Respectfully, National Security Service of the Republic of Armenia.” A blue button labelled “VIEW FILES” follows, with a note recommending Adobe Acrobat Reader.

DOCUMENTED. The button is a link annotation whose action is JavaScript: this.exportDataObject({ cName: 'NSS_FILES_Diaspora.rar' }). This prompts the reader to save the embedded file. The attachment’s filename ends in an invisible zero-width space (U+200B), and its embedded-file record carries creation and modification dates of 22 September 2026.

ASSESSMENT. The Acrobat recommendation is operational, not cosmetic: exportDataObject is supported in Acrobat but not in most browser-based viewers. The empty-password encryption likely serves to hinder editing and to complicate some automated scanners. The zero-width character is likely intended to defeat extension-based filtering.

3. Infection Chain

3.1 Stage 0 — Dropped archive NSS_FILES_Diaspora.rar

DOCUMENTED. RAR5 archive containing a folder NSS_202603068113 with four files:

- 2-Lori_Ugurluoglu-C28ECEAD5EC7C54E96181C77401B.pdf — genuine-appearing CV (decoy, clean; Ghostscript re-render dated 19 Sep 2026).
- Edmond Bejanian-E61E25EEF4352C5AFA69.docx — genuine-appearing Europass CV (decoy; no macros, remote templates or OLE objects).
- Passport3-C4622915D3F28FD1003B521461A1.png — image of an identity document (decoy).
- SarkisBelian-PDF-63DAACCD63926BAE983768OXSNNNXN.exe — malicious executable named to look like a PDF.

ASSESSMENT. The decoys appear to be real personal documents of diaspora-linked professionals, most likely obtained from an earlier compromise or an application or registration dataset. The individuals named are therefore also affected parties.

3.2 Stage 1 — WinRAR SFX (SarkisBelian-PDF-….exe)

DOCUMENTED. PE32+ WinRAR self-extracting module (PDB path D:\Projects\WinRAR\SFX\build\sfxrar64\Release\sfxrar.pdb; unsigned). The overlay archive's SFX script, padded with blank lines to hide it in the archive comment, is: Path=%temp%\ ; Setup=%temp%\SNDCJPXMKSUDZPAOSOXSNNNXN.exe -pVOVA ; Setup=%temp%\SarkisBelian.pdf ; Silent=1 ; Overwrite=1. It therefore opens a genuine CV (SarkisBelian.pdf) as a distraction while launching the next stage with the archive password VOVA.

3.3 Stage 2 — Password-protected WinRAR SFX (SNDCJPXMKSUDZPAOSOXSNNNXN.exe)

DOCUMENTED. Second WinRAR SFX, AES-encrypted with password VOVA. It extracts to %APPDATA%\deploy_my\ and runs AutoIt3.exe /AutoIt3ExecuteLine "Run("%appdata%\deploy_my\a.cmd", @ScriptDir, @SW_HIDE)". Contents: a legitimate AutoIt3 interpreter with stock include files, curl.exe and libcurl.dll (two copies each), a.cmd, killit.ps1 and soft4.ps1.

DOCUMENTED. File timestamps in this stage show a.cmd (12 Jun 2026), killit.ps1 (4 Jun 2026) and curl (3 Jun 2026) predating the campaign build, while soft4.ps1 was rebuilt on 19 September 2026.

ASSESSMENT. The toolkit has been in development or use since at least June 2026, and this lure represents a later deployment rather than a first build.

3.4 Persistence — a.cmd

DOCUMENTED. The batch file, obfuscated with junk lines, creates two scheduled tasks, both launched through AutoIt so that no PowerShell window appears:

- GRE — every 3 minutes: powershell.exe -ep bypass -WindowStyle Hidden -Command %appdata%\deploy_my\soft4.ps1 VOVA ABC
- GRELK — every 29 minutes: runs killit.ps1, which force-kills any PowerShell process whose command line contains “ABC”.

ASSESSMENT. The pair works as a watchdog: GRELK periodically terminates the implant and GRE relaunches it within three minutes, recovering from hung sessions. The implant’s own single-instance check (below) prevents duplicates between restarts.

3.5 Loader — soft4.ps1

DOCUMENTED. The script takes its key from the first argument (VOVA), pads it to 32 bytes with 0xAA, and decrypts a 240-chunk base64 blob with AES-CBC (IV DsF65rwaNlBEnd8CjNlrZQ==). The result is a further script labelled “INTERMEDIATE OBFUSCATION – Iteration 2”, which unwraps two base64 layers before running the final implant via [scriptblock]::Create.

ASSESSMENT. The iteration labels indicate a scripted obfuscation builder, so future samples are likely to vary in their wrapping while the core implant stays the same.

4. Final Implant Capabilities

DOCUMENTED. On start, the implant writes a victim identifier (a GUID reformatted as XXXXXX-XXXXX-XXXXX-XXXXX-XXXXX) to id.txt beside the script. It exits if another PowerShell or pwsh process carries the ABC marker, and fetches curl from the C2 if absent. It then loops indefinitely: it GETs https://conference.sources-debian[.]info/tasks.php?GUID=<id>, executes the command, uploads results to /upload.php?GUID=<id>, takes and uploads a screenshot, and sleeps for a random 10–20 seconds. All traffic uses curl with -k (certificate validation disabled) and a spoofed Firefox user-agent.

Command set recovered from the code:

- **massdownload|<dir>|<ext>** — recursively uploads every matching file, then a file listing (list.txt).
- **searchfname|<dir>|<pattern>** — returns matching file paths (matches__*.dat).
- **upload|<path>** — exfiltrates a single file.
- **zip|<path>** — fetches 7z.exe/7z.dll from /tools/archive/, splits the target into 2 MB volumes and uploads each part.
- **unzip|<zip>|<dir>** — unpacks a staged archive on the host and reports a directory listing.
- **download|<url>|<dir>** — writes an arbitrary file from any URL to disk (further payload delivery).
- **portscan|<ip>|<ports>** — fetches /tools/sc/scan.ps1 and scans internal hosts; the report is uploaded.
- **tunnel|<server>|<port>|<user>|<pass>|<lip>|<lport>|<vpsport>** — fetches plink.exe from /tools/tun/ and opens a reverse SSH port-forward from an attacker VPS into the victim network.
- **screenshot|1** — on-demand screenshot (one is also taken on every loop).

- **any other string** — executed via cmd.exe /c; the output is uploaded.

ASSESSMENT. Screenshots every 10–20 seconds amount to near-continuous visual surveillance of an infected workstation, capturing messaging, documents and credentials typed on screen. The port-scan and tunnel functions indicate intent to move beyond the first machine into the victim's organisation.

5. Infrastructure

DOCUMENTED. C2 hostname conference.sources-debian[.]info. Registration-age data provided by Malwarebytes indicates the parent domain has existed for about 2 years 3 months (registered around mid-2024); registrant data is not public and the .info WHOIS query returned no details. Malwarebytes returned verdict "unknown". A web search found no public reporting on the domain.

ASSESSMENT. The name imitates Linux package-mirror infrastructure ("sources", "debian") and uses a "conference" subdomain, both chosen to look benign in proxy logs. The domain age suggests it was registered well before this campaign and may have been used in earlier operations.

HYPOTHESIS. The same server may host operator tooling (/tools/curl/, /tools/archive/, /tools/sc/, /tools/tun/) shared across other campaigns. This was not tested, to avoid alerting the operator.

6. Targeting and Attribution

ASSESSMENT. The lure targets the Armenian diaspora and organisations working with it. Supporting evidence: the filename ("for Armenian Diaspora"), the folder and attachment naming (NSS_FILES_Diaspora), the choice of decoys (diaspora-linked professionals in the UAE, Iran and Armenia), and Armenian-language text addressed to "colleagues". Impersonating the NSS is intended to exploit deference to state authority, and may also aim to damage trust between the diaspora and Armenian institutions.

ASSESSMENT. The combination of a state-impersonation social-engineering lure, curated personal-document decoys, a hand-built modular espionage implant, internal reconnaissance and tunnelling, and no monetisation mechanism points to espionage rather than crime.

HYPOTHESIS. The operator string "VOVA" (a Russian diminutive of Vladimir) is used as both archive password and AES key. It is weak evidence of operator language and may be deliberate misdirection; it should not be used for attribution on its own. No overlap with publicly documented Armenia-targeting clusters has yet been established.

7. MITRE ATT&CK Mapping

- T1566.001 Phishing: Spearphishing Attachment (assumed delivery vector)
- T1204.002 User Execution: Malicious File
- T1036.008 / T1036.007 Masquerading: file-type masquerade ("-PDF-….exe") and zero-width character in attachment name
- T1027 / T1027.013 Obfuscated Files or Information: encrypted/encoded file (AES + nested base64, SFX script padding, junk-line batch)
- T1140 Deobfuscate/Decode Files or Information

- T1059.001 / T1059.003 / T1059.010 Command and Scripting Interpreter: PowerShell, Windows Command Shell, AutoHotKey & AutoIT
- T1053.005 Scheduled Task/Job: Scheduled Task (GRE, GRELK)
- T1564.003 Hide Artifacts: Hidden Window
- T1113 Screen Capture
- T1083 File and Directory Discovery; T1119 Automated Collection; T1005 Data from Local System
- T1560.001 Archive Collected Data: Archive via Utility (7-Zip, 2 MB volumes)
- T1071.001 Application Layer Protocol: Web Protocols; T1041 Exfiltration Over C2 Channel
- T1105 Ingress Tool Transfer (curl, 7z, plink, scan.ps1)
- T1046 Network Service Discovery (portscan)
- T1572 Protocol Tunneling (plink reverse SSH)

8. Indicators of Compromise

> C2 domains are defanged. SHA-256 unless stated. Decoy files are included for detection and for victim identification; they are not malicious in themselves.

8.1 Files

- **Lure PDF — Hovel Chernokian SNS CASE for Armenian Diaspora.pdf:** 84aa7a7dfcebe5d80dd0911393d0154d3320fa009d591bff2ca32af8d019f106 (MD5 bf4cfbe5a919339de227e1638293d743)
- **NSS_FILES_Diaspora.rar:** 8cc7a1325cc31871a311faf2e05ca8835515358d2fe3a5625544998b76e6e6e8 (MD5 1baaf53c8a1a0b0eb65a54b07908b759)
- **SarkisBelian-PDF-63DAACCD63926BAE983768OXSNNNXN.exe (stage 1 SFX):** f6764bd4d87ef804eb704ae38370613a02b949744b6ddec92095ae7888c113c6 (MD5 e48cc7241b1b6f007354269b36290972)
- **SNDCJPXMKSUDZPAOSOXSNNNXN.exe (stage 2 SFX):** 4e2378348ebbac20735896a188d021d2dce0b984cd74ec97d620bb43a3d42cd8
- **soft4.ps1 (encrypted loader):** e26faa9ae181d08579ff2d4c5fb99cc65174338a4dec9f1f84b0253135cb31d7
- **Decrypted intermediate script:** feb48a99b86c91e40bff2c0d78e282e05e9024e7baa17a963b15824c28e0beab
- **a.cmd (persistence):** 4fd12b05d71572659947ab04b03d25a30f855024d27481359af02669e45896d2
- **killit.ps1 (watchdog):** dc7e3152de5e6616af748dcd87a3170a0244b41343418f061c670732049c62cf
- **curl.exe (legitimate, abused):** 104f9f7f400e8231198d240897b44fed8b43057a85b183314699d3c3898b6766
- **libcurl.dll (legitimate, abused):** 988795cb4e2dbe703d9a1ab3c7d7b76e431bcdafdba2a293582ad40f4f9607a1

- **AutoIt3.exe (legitimate, abused):** 98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b
- **Decoy SarkisBelian.pdf:** 1daa8010c8638d89d9a47b0982851e9d9e43490b3da5969ddeed0151ee0694bf
- **Decoy 2-Lori_Ugurluoglu-….pdf:** a7b37ec3dadc7f34d10236744c6b48329b7ea951983710975a540357f1eff5d8
- **Decoy Edmond Bejanian-….docx:** 7811dba6f20a50f7e086db60d223993cbc36c078e24088b58625272e1192d709
- **Decoy Passport3-….png:** 31a16091f1c299155ae4b9abb39a3ba4b9a759174ff1eb68c16099c4823ac7a2

8.2 Network

- conference.sources-debian[.]info
- hxxps://conference.sources-debian[.]info/tasks.php?GUID=
- hxxps://conference.sources-debian[.]info/upload.php?GUID= (also &mssdownload=1)
- /tools/curl/curl.exe, /tools/curl/libcurl.dll, /tools/archive/7z.exe, /tools/archive/7z.dll, /tools/sc/scan.ps1, /tools/tun/plink.exe
- User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:134.0) Gecko/20100101 Firefox/138.0 (the rv/Firefox version mismatch is a useful detection anchor)

8.3 Host

- Directory %APPDATA%\deploy_my\ (with AutoIt3\ subfolder and id.txt)
- Scheduled tasks named GRE and GRELK
- powershell.exe command line containing “-ep bypass -Windowstyle Hidden -Command”, “soft4.ps1 VOVA ABC”
- AutoIt3.exe with /AutoIt3ExecuteLine spawning cmd.exe or powershell.exe
- %TEMP%\SNDCJPXMKSUDZPAOSOXSNNNXN.exe, %TEMP%\SarkisBelian.pdf, %TEMP%\list.txt, %TEMP%\<guid>\screen_####.jpg, %TEMP%\matches__*.dat, %TEMP%\ScanReport_*.txt
- Strings: VOVA; IV DsF65rwaNlBEnd8CjNlrZQ==; “INTERMEDIATE OBFUSCATION - Iteration”

9. Detection and Response Recommendations

- Block conference.sources-debian[.]info and the parent domain at DNS, proxy and firewall. Retro-hunt DNS and proxy logs from June 2026 onward.
- Hunt for scheduled tasks GRE/GRELK, the %APPDATA%\deploy_my path, and AutoIt3.exe running from user-writable directories.
- Alert on the spoofed user-agent string and on curl.exe with -k from non-developer endpoints.
- For any confirmed infection: isolate the host and preserve memory and disk. Delete the tasks and folder only after imaging. Rotate all credentials from a clean device, and treat everything shown on

screen or stored locally since infection as compromised. If the tunnel command may have been used, review internal network logs for reverse SSH.

- Disable JavaScript in Adobe Acrobat/Reader (Preferences › JavaScript) for at-risk users; the lure depends on it.
- Brief diaspora organisations and partner communities: the NSS does not distribute case files as PDF attachments with a “view files” button.
- Notify the individuals whose CVs and identity document were used as decoys; their data is in adversary hands.
- Share IOCs with CERT.AM and the NSS, and submit samples to relevant vendors for detection coverage.

10. Analytic Gaps

- The delivery vector (email, messenger, social media) and the recipient set are unknown.
- The server-side tasking and the contents of /tools/sc/scan.ps1 were not retrieved.
- Number of victims and victim geography: unknown.
- No infrastructure pivoting (passive DNS, certificate history, hosting) was performed for this note; this is the priority next step.

References

- MITRE ATT&CK, T1053.005 Scheduled Task. https://attack.mitre.org/techniques/T1053/005/
- MITRE ATT&CK, T1059.010 AutoHotKey & AutoIT. https://attack.mitre.org/techniques/T1059/010/
- MITRE ATT&CK, T1113 Screen Capture. https://attack.mitre.org/techniques/T1113/
- MITRE ATT&CK, T1572 Protocol Tunneling. https://attack.mitre.org/techniques/T1572/
- MITRE ATT&CK, T1036 Masquerading. https://attack.mitre.org/techniques/T1036/
- Adobe, Acrobat JavaScript API — Doc.exportDataObject. https://opensource.adobe.com/dc-acrobat-sdk-docs/library/jsapiref/doc.html