INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-02 14:02 UTC

SideCopy/APT36 Operation XENOFISCAL: Xeno RAT 1.8.7 Targets Afghan Finance Ministry; DeskRAT Golang ELF Implant Targets Indian Military

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0393
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Windows systems (LNK, mshta.exe, registry persistence), Afghanistan Ministry of Finance and provincial revenue directorates; Linux systems (.desktop files, Golang ELF implant), Indian military and defense personnel
Published	2026-06-02T05:05:40
Discovery Source	Rss

Executive Summary

Pakistan-linked threat group SideCopy (APT36/Transparent Tribe) is running simultaneous espionage operations against Afghanistan's Ministry of Finance and Indian military personnel. The Windows-track campaign delivers Xeno RAT 1.8.7 via spear-phishing LNK files; the Linux-track deploys a new Golang implant called DeskRAT through weaponized .desktop files. Both tracks are designed to steal credentials, capture screens, and record keystrokes - capabilities that enable theft of sensitive government fiscal data and military communications by a state-aligned adversary.

Technical Analysis

SideCopy/APT36 is executing a dual-platform espionage campaign with no associated CVEs; exploitation relies entirely on social engineering and native OS feature abuse. Windows track (Operation XENOFISCAL): spear-phishing delivers malicious LNK files (T1566.001, T1204.002) that invoke mshta.exe for fileless HTA execution (T1218.005), download and execute Xeno RAT 1.8.7 (T1105), and establish registry Run key persistence (T1547.001). Xeno RAT capabilities include clipboard capture (T1115), keylogging (T1056.001), screen capture (T1113), video capture (T1125), process enumeration (T1057), file discovery (T1083), C2 over HTTP/HTTPS (T1071.001), and internal proxy (T1090.001). Linux track: weaponized .desktop files (T1036.004, T1608.004) execute a previously undocumented Golang ELF implant, DeskRAT, targeting Indian military

personnel. DeskRAT uses DLL side-loading equivalent techniques (T1574.002) and obfuscation (T1027). Both tracks use scheduled tasks or equivalent persistence (T1053.005) and Windows Command Shell or JavaScript (T1059.003, T1059.007). Relevant CWEs: CWE-494 (download of code without integrity check), CWE-693 (protection mechanism failure), CWE-601 (open redirect, relevant to C2 proxying). No patches are applicable; the attack surface is user behavior and OS configuration. Attribution confidence is medium per available vendor analysis (CYFIRMA, SOC Prime); attribution to Pakistan-linked actors relies on TTP correlation and targeting patterns.

Action Checklist

1. Step 1: Containment, Block execution of mshta.exe for non-administrative users via AppLocker or Windows Defender Application Control (WDAC) policies; audit .desktop files in user-writable directories (~/.local/share/applications/, ~/.config/autostart/) for suspicious entries and where operationally feasible, restrict execution of .desktop files to verified package manager-installed entries. Isolate any Windows host where mshta.exe spawned a child process not originating from a browser. Priority targets: systems used by personnel with access to financial, procurement, or defense data.
2. Step 2: Detection, Hunt for mshta.exe spawning PowerShell, cmd.exe, or network connections (Event ID 4688 with process lineage; Sysmon Event ID 1/3). Search endpoint logs for LNK files executed from user Downloads, Temp, or email attachment directories. On Linux, audit .desktop files in ~/.local/share/applications/ and /etc/xdg/autostart/ for entries referencing non-standard executables or base64-encoded commands. Query EDR for Golang ELF binaries with no package manager provenance (CIS 2.1). Cross-reference outbound HTTP/HTTPS connections to uncategorized or newly registered domains (NIST AU-6).
3. Step 3: Eradication, Remove malicious LNK files and any dropped Xeno RAT binaries; purge associated registry Run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run). On Linux, remove unauthorized .desktop files and the DeskRAT ELF binary. Revoke and rotate credentials for any user account on an affected host (per MITRE D3 practices). Disable or restrict mshta.exe at the application control layer (NIST CM-7, CIS 4.6). Enforce NIST SI-4 continuous monitoring to confirm no residual C2 beaconing post-cleanup.
4. Step 4: Recovery, Re-image confirmed-compromised hosts where forensic analysis cannot rule out persistent implant staging. Validate registry Run keys and scheduled tasks (T1053.005) are clean before returning systems to production. Monitor outbound network traffic for 30 days post-remediation for low-and-slow C2 patterns on HTTP/HTTPS (NIST AU-6, NIST SC-7). Confirm MFA is enforced on all accounts that authenticated from affected hosts (CIS 6.3, CIS 6.5, MITRE D3 Multi-Factor Authentication) before restoring access.
5. Step 5: Post-Incident, Conduct a gap assessment against NIST SI-3 (malicious code protection) and NIST SI-4 (system monitoring) for LNK and HTA execution visibility. Enforce NIST AC-6 (least privilege) to prevent mshta.exe access for standard users. Review and update spear-phishing awareness training specific to LNK and .desktop file lures (NIST AT-2). Evaluate whether MITRE ATT&CK coverage for T1218.005 (mshta.exe), T1547.001 (registry persistence), and T1036.004 (masquerading via .desktop files) exists in current detection rule sets; if not, develop and tune them (NIST SI-4, CIS 8.2).

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to national CERT or government CISO if forensic evidence confirms successful credential exfiltration from Ministry of Finance fiscal systems or Indian military endpoints, if Xeno RAT C2 communications are confirmed active, or if DeskRAT ELF persistence is identified on classified network segments — all of which constitute nation-state espionage incidents requiring inter-agency coordination beyond standard IR team authority.
Recovery Notes	Before restoring any Afghan Ministry of Finance or Indian military endpoint to production, obtain a written sign-off from the CISO or equivalent authority confirming that Autoruns analysis, registry baseline comparison, and 72-hour post-eradication Sysmon log review all show no residual Xeno RAT 1.8.7 or DeskRAT artifacts. Monitor all recovered hosts for 30 days using daily Sysmon Event ID 3 log review for low-and-slow HTTP/HTTPS beaconing to newly registered domains, as APT36 campaigns have historically used fallback C2 channels that activate after primary C2 disruption. Treat any credential that authenticated on a confirmed-compromised host as fully compromised — rotate all associated passwords and API keys and enforce MFA before any account is restored, given Xeno RAT's documented keylogging and credential harvesting capabilities.
Forensic Artifacts	Windows Security Event Log Event ID 4688 entries with ParentProcessName=mshta.exe and NewProcessName=powershell.exe or cmd.exe — these establish the SideCopy HTA-to-RAT staging chain specific to Xeno RAT 1.8.7 delivery | Malicious LNK files in %USERPROFILE%\Downloads, %TEMP%, or Outlook attachment cache directories — LNK forensics (using LNKParse3 or LECmd) will reveal the target executable path, working directory, and creation timestamp tied to the SideCopy spear-phishing campaign | HKCU\Software\Microsoft\Windows\CurrentVersion\Run registry values created or modified within the incident window — Xeno RAT 1.8.7 uses this key for persistence and the value name will typically mimic a legitimate software entry to evade casual inspection | DeskRAT Golang ELF binary located in non-standard paths such as ~/.config/, /tmp/, or /var/tmp/ on Linux endpoints — 'strings' output will contain Golang build metadata including GOPATH and module paths that provide APT36 infrastructure attribution | Network capture (pcap) of outbound HTTP/HTTPS sessions from affected hosts showing periodic low-volume beaconing intervals — Xeno RAT C2 traffic patterns and DeskRAT beacon timing are distinct from legitimate application traffic and will appear in Wireshark as regular interval connections to uncategorized or newly registered domains

Per-Action IR Details

Step 1: Containment — Block execution of mshta.exe for non-administrative users via AppLocker or Windows Defender Application Control (WDAC) policies; restrict .desktop file execution on Linux hosts to verified package manager-installed entries only. Isolate any Windows host where mshta.exe spawned a child process not originating from a browser. Priority targets: systems used by personnel with access to financial, procurement, or defense data.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy

Controls: NIST CM-7 (Least Functionality) — deny-list or restrict mshta.exe execution via WDAC publisher rules, NIST AC-3 (Access Enforcement) — enforce application control decisions at the OS layer for non-admin users, NIST IR-4 (Incident Handling) — execute containment actions per the documented IR plan, CIS 4.4 (Implement and Manage a Firewall on Servers) — block outbound C2 ports from isolated hosts, CIS 4.6 (Securely Manage Enterprise Assets and Software) — enforce application allowlisting to prevent mshta.exe and unsigned ELF execution

Compensating: Without enterprise WDAC management, deploy a Software Restriction Policy (SRP) via Local Group Policy (gpedit.msc → Computer Configuration → Windows Settings → Security Settings → Software Restriction

Policies) to hash-deny mshta.exe (SHA-256: verify against known-clean copy). On Linux, use chmod 000 /usr/bin/mshta or equivalent; audit ~/.local/share/applications/ with 'find ~/.local/share/applications /etc/xdg/autostart -name "*.desktop" -newer /var/log/dpkg.log' to flag entries not installed via apt/yum. Network-isolate affected hosts using host-based Windows Firewall rules: 'netsh advfirewall firewall add rule name="Block Xeno RAT C2" dir=out action=block program="%APPDATA%\[suspicious_path]"' once binary path is identified.

Evidence: Before isolating, capture a full memory image using WinPmem or DumpIt on Windows hosts where mshta.exe spawned anomalous children — volatile memory will contain the in-memory Xeno RAT 1.8.7 payload, decrypted C2 configuration, and active network socket state. On Linux, run 'ss -tulnp' and 'ls -la /proc/[pid]/exe' to capture DeskRAT ELF process details and resolve the binary path before the process is killed. Snapshot the full registry hive HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnce using 'reg export HKCU\Software\Microsoft\Windows\CurrentVersion\Run C:\evidence\runkeys.reg' to preserve Xeno RAT persistence entries prior to removal.

Step 2: Detection — Hunt for mshta.exe spawning PowerShell, cmd.exe, or network connections (Event ID 4688 with process lineage; Sysmon Event ID 1/3). Search endpoint logs for LNK files executed from user Downloads, Temp, or email attachment directories. On Linux, audit .desktop files in ~/.local/share/applications/ and /etc/xdg/autostart/ for entries referencing non-standard executables or base64-encoded commands. Query EDR for Golang ELF binaries with no package manager provenance (CIS 2.1). Cross-reference outbound HTTP/HTTPS connections to uncategorized or newly registered domains (NIST AU-6).

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — review Windows Security and Sysmon logs for mshta.exe process lineage indicative of Xeno RAT staging, NIST AU-2 (Event Logging) — ensure Event ID 4688 (Process Creation) with command-line auditing enabled to capture mshta.exe child process arguments, NIST SI-4 (System Monitoring) — monitor for DeskRAT ELF beacon patterns and LNK execution from non-standard directories, CIS 2.1 (Establish and Maintain a Software Inventory) — identify Golang ELF binaries absent from package manager database as anomalous, CIS 8.2 (Collect Audit Logs) — ensure audit logs from Windows Security Event Log and Linux auditd are centrally collected for correlation

Compensating: Without a SIEM, run this Sysmon-based PowerShell hunt locally: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Id -in 1,3 -and $_.Message -match "mshta.exe"} | Select-Object TimeCreated, Message | Export-Csv C:\evidence\mshta_hunt.csv'. For LNK file discovery, run: 'Get-ChildItem -Path $env:USERPROFILE\Downloads, $env:TEMP -Recurse -Filter "*.lnk" | Select-Object FullName, CreationTime, LastWriteTime | Export-Csv C:\evidence\lnk_files.csv'. On Linux, deploy osquery with this query: 'SELECT name, path, cmdline FROM processes WHERE cmdline LIKE "%base64%" OR name LIKE "%.elf"' and audit with 'grep -r "Exec=" ~/.local/share/applications/ /etc/xdg/autostart/ | grep -v "/usr/bin\|/usr/lib"'. Use Sigma rule for mshta.exe parent-child detection (SigmaHQ rule: proc_creation_win_mshta_spawn_shell) converted to Windows Event Log query via sigmac.

Evidence: Preserve Windows Security Event Log Event ID 4688 entries showing mshta.exe parent-child relationships (filter: ParentProcessName contains 'mshta.exe' AND NewProcessName contains 'powershell.exe' or 'cmd.exe') — these establish the HTA execution chain SideCopy uses to stage Xeno RAT 1.8.7. Collect Sysmon Event ID 3 (Network Connection) records for mshta.exe showing external destination IPs and ports, which will reveal the Xeno RAT C2 endpoint. On Linux, collect 'find / -name "*.desktop" -newer /etc/passwd -ls 2>/dev/null' output and hash all returned files with sha256sum — DeskRAT delivery via .desktop file will show a recently created entry with an Exec= line referencing a binary in a non-standard path (e.g., ~/.config/, /tmp/). Capture browser and email client download history to establish the LNK spear-phishing delivery vector and sender attribution.

Step 3: Eradication — Remove malicious LNK files and any dropped Xeno RAT binaries; purge associated registry Run keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run). On Linux, remove unauthorized .desktop files and the DeskRAT ELF binary. Revoke and rotate credentials for any user account on an affected

host (D3-CRO). Disable or restrict mshta.exe at the application control layer (NIST CM-7, CIS 4.6). Enforce NIST SI-4 continuous monitoring to confirm no residual C2 beaconing post-cleanup.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST CM-7 (Least Functionality) — disable mshta.exe via WDAC or AppLocker deny rule as a permanent control, not just incident-scoped, NIST SI-2 (Flaw Remediation) — remove Xeno RAT binaries and DeskRAT ELF implant and verify removal against known file hashes, NIST AC-2 (Account Management) — disable and rotate credentials for all accounts that authenticated on confirmed-compromised hosts, NIST SI-4 (System Monitoring) — validate C2 beaconing has ceased using network monitoring post-eradication, CIS 4.6 (Securely Manage Enterprise Assets and Software) — enforce application allowlist to prevent Xeno RAT re-execution from any residual dropper, CIS 5.3 (Disable Dormant Accounts) — disable accounts used on compromised hosts pending credential rotation and verification

Compensating: Verify Xeno RAT binary removal by computing SHA-256 hashes of all executables in %APPDATA%, %TEMP%, and %ProgramData% and comparing against VirusTotal or a locally curated YARA rule targeting Xeno RAT 1.8.7 strings (hunt for strings: 'XenoRat', 'xeno_rat', Golang build artifacts in the ELF binary). Run: 'Get-ChildItem -Path $env:APPDATA, $env:TEMP, $env:ProgramData -Recurse -Include "*.exe","*.dll" | Get-FileHash -Algorithm SHA256 | Export-Csv C:\evidence\binary_hashes.csv'. For registry cleanup verification: 'Get-ItemProperty -Path "HKCU:\Software\Microsoft\Windows\CurrentVersion\Run" | Format-List' and 'Get-ScheduledTask | Where-Object {$_.TaskPath -notlike "\Microsoft*"} | Export-Csv C:\evidence\scheduled_tasks.csv'. On Linux, use ClamAV with a custom signature for DeskRAT Golang ELF artifacts: 'clamscan -r /home /tmp /var/tmp --log=/var/log/clamscan_deskrat.log'.

Evidence: Before purging registry Run keys, export the full hive for forensic preservation: 'reg export HKCU C:\evidence\HKCU_full.reg' — Xeno RAT 1.8.7 is known to use Run key persistence and may use obfuscated value names mimicking legitimate software. Collect the malicious LNK files with metadata intact (do not open) using 'Copy-Item -Path "C:\Users*\Downloads*.lnk" -Destination C:\evidence\lnk_artifacts\' — LNK file forensics will reveal the target path, working directory, and icon resource used by SideCopy for social engineering. On Linux, preserve the DeskRAT ELF binary with 'cp /path/to/deskrat /evidence/deskrat.elf && sha256sum /evidence/deskrat.elf' before deletion — Golang ELF binaries retain embedded build metadata (GOPATH, module paths) that can provide infrastructure attribution for the APT36 campaign.

Step 4: Recovery — Re-image confirmed-compromised hosts where forensic analysis cannot rule out persistent implant staging. Validate registry Run keys and scheduled tasks (T1053.005) are clean before returning systems to production. Monitor outbound network traffic for 30 days post-remediation for low-and-slow C2 patterns on HTTP/HTTPS (NIST AU-6, NIST SC-7). Confirm MFA is enforced on all accounts that authenticated from affected hosts (CIS 6.3, CIS 6.5, D3-MFA) before restoring access.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting) — conduct daily review of outbound HTTP/HTTPS connections from recovered hosts for 30 days, specifically for low-volume periodic beaconing patterns consistent with Xeno RAT C2 check-in intervals, NIST SC-7 (Boundary Protection) — enforce egress filtering at the network perimeter to block connections to newly registered or uncategorized domains that Xeno RAT C2 infrastructure typically uses, NIST CP-10 (System Recovery and Reconstitution) — restore from verified clean backup or re-image; do not restore from a backup taken after the estimated initial compromise date, CIS 6.3 (Require MFA for Externally-Exposed Applications) — enforce MFA on all web portals and remote access used by personnel whose credentials may have been harvested by Xeno RAT's keylogging module, CIS 6.5 (Require MFA for Administrative Access) — require MFA for all admin accounts that were active on compromised Ministry of Finance or Indian military endpoints

Compensating: For 30-day post-recovery C2 monitoring without a SIEM, configure Sysmon Event ID 3 to log all outbound connections from recovered hosts and run a nightly PowerShell script to flag connections to domains registered within the past 90 days: 'Get-WinEvent -LogName "Microsoft-Windows-Sysmon/Operational" | Where-Object {$_.Id -eq 3} | Select-Object TimeCreated, @{n="Dest";e={$_.Properties[14].Value}} | Export-Csv

C:\monitoring\daily_connections_$(Get-Date -Format yyyyMMdd).csv'. Use Wireshark or tcpdump with a capture filter for HTTP User-Agent strings associated with Xeno RAT ('tcpdump -i eth0 -w /pcaps/recovery_monitor_$(date +%Y%m%d).pcap host [recovered_host_ip]') and review weekly. For scheduled task validation: 'schtasks /query /fo LIST /v | findstr /i "Task Name\|Run As User\|Task To Run"' and compare against a known-good baseline.

Evidence: Before returning any host to production, run Autoruns (Sysinternals) with 'autorunsc.exe -accepteula -a * -c -h -o C:\evidence\autoruns_final.csv' and diff against a clean baseline — Xeno RAT 1.8.7 and APT36 tooling commonly establish multiple persistence mechanisms (Run keys, scheduled tasks, COM hijacking) so a single registry key removal is insufficient to confirm clean state. Collect a final Sysmon log snapshot covering the 72 hours post-eradication and verify absence of mshta.exe execution events or outbound connections to the previously identified Xeno RAT C2 domains/IPs before signing off on recovery. Document the verified-clean state with timestamps for regulatory and leadership reporting, as Afghan Ministry of Finance and Indian defense sector incidents may trigger government incident disclosure obligations.

Step 5: Post-Incident — Conduct a gap assessment against NIST SI-3 (malicious code protection) and NIST SI-4 (system monitoring) for LNK and HTA execution visibility. Enforce NIST AC-6 (least privilege) to prevent mshta.exe access for standard users. Review and update spear-phishing awareness training specific to LNK and .desktop file lures (NIST AT-2). Evaluate whether MITRE ATT&CK coverage for T1218.005 (mshta.exe), T1547.001 (registry persistence), and T1036.004 (masquerading via .desktop files) exists in current detection rule sets — if not, develop and tune them (NIST SI-4, CIS 8.2).

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity

Controls: NIST SI-3 (Malicious Code Protection) — assess whether endpoint protection detected Xeno RAT 1.8.7 or DeskRAT on delivery; if not, evaluate signature/behavioral rule gaps and submit samples to AV vendor, NIST SI-4 (System Monitoring) — develop detection rules specifically for mshta.exe (T1218.005) parent-child chains and Golang ELF beaconing patterns characteristic of DeskRAT, NIST AC-6 (Least Privilege) — enforce mshta.exe execution restriction for all non-admin users as a permanent control emerging from this incident, NIST AU-2 (Event Logging) — verify that process creation command-line logging (Event ID 4688) and Sysmon are deployed and collecting on all endpoints that were in scope for this campaign, CIS 8.2 (Collect Audit Logs) — ensure Linux auditd rules capture .desktop file execution and ELF binary execution from non-standard paths across all Linux endpoints used by defense personnel, CIS 7.1 (Establish and Maintain a Vulnerability Management Process) — incorporate LNK and .desktop file weaponization as a recurring threat scenario in the vulnerability management review cycle

Compensating: For detection rule development without commercial SIEM, implement these specific Sigma rules from SigmaHQ: 'proc_creation_win_mshta_spawn_shell.yml' (T1218.005), 'registry_run_keys_startup_folder.yml' (T1547.001), and write a custom Sigma rule for .desktop file Exec= anomalies targeting T1036.004. Convert rules to Windows Event Log queries using sigmac: 'sigmac -t windows-eventlog proc_creation_win_mshta_spawn_shell.yml'. Deploy a YARA rule scanning for Xeno RAT 1.8.7 strings and Golang ELF build metadata as a scheduled weekly scan using ClamAV custom signatures. For awareness training, create a simulated LNK spear-phishing exercise using a benign payload that mimics an Afghan Finance Ministry document lure — the same social engineering pretext SideCopy used in this campaign.

Evidence: Compile a lessons-learned artifact package containing: the original malicious LNK file metadata (target path, working directory, creation timestamp, icon resource path) to support future phishing simulations; DeskRAT ELF binary with extracted Golang build metadata (use 'strings deskrat.elf | grep -E "go/src|github.com|golang"') to identify APT36 infrastructure patterns; and a timeline mapping the kill chain from LNK execution through mshta.exe staging to Xeno RAT C2 establishment using correlated Sysmon Event IDs 1, 3, and 11 — this timeline becomes the evidentiary basis for detection rule validation and ATT&CK technique coverage gap closure.

Detection Guidance

Windows: Alert on mshta.exe (Event ID 4688 / Sysmon EID 1) with parent processes including explorer.exe, outlook.exe, or any mail client; flag any child network connections from mshta.exe (Sysmon EID 3). Hunt for

LNK files in user-writable directories (Downloads, AppData\Temp) with creation timestamps within the last 30 days executing external commands. Check for new registry Run key entries (Event ID 13 in Sysmon) pointing to non-standard binary paths. Hunt for Xeno RAT indicators: processes establishing persistent outbound HTTP/HTTPS connections to uncategorized domains, especially with low byte-count beacons. Linux: Search for .desktop files outside /usr/share/applications/ or installed package paths, particularly those containing Exec= entries with paths to /tmp/, /home/, or base64-encoded commands. Look for Golang ELF binaries (identifiable by 'go build' metadata strings) with no corresponding package manager record. Monitor for outbound connections from these binaries to infrastructure not in your baseline. General: Apply YARA or EDR behavioral rules for T1218.005 (mshta.exe abuse), T1547.001 (Run key writes), and T1036.004 (masqueraded file types). SOC Prime has published detection content for this campaign; validate detection rules against your SIEM and incident data before deployment. T3 vendor sources are reputable but should be corroborated with your environment. Confidence in specific IOC values from current sources is medium; treat hashes and domains as indicators requiring corroboration, not definitive blocklist entries.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`Not publicly confirmed in T3 sources at time of reporting`	Xeno RAT 1.8.7 binary hashes referenced in CYFIRMA and SOC Prime reporting but not reproduced in available source content — obtain directly from those advisories	LOW
HASH	`Not publicly confirmed in T3 sources at time of reporting`	DeskRAT Golang ELF implant hash not confirmed in available source content — obtain directly from CYFIRMA advisory	LOW
URL	`Not confirmed`	C2 infrastructure URLs not reproduced in available source content — consult SOC Prime active threats entry for campaign-specific domains	LOW

Framework Mappings

MITRE-ATTACK

- **T1036.004** — Masquerade Task or Service
- **T1608.004** — Drive-by Target
- **T1115** — Clipboard Data
- **T1574.002** — DLL Side-Loading
- **T1090.001** — Internal Proxy
- **T1083** — File and Directory Discovery
- **T1057** — Process Discovery
- **T1041** — Exfiltration Over C2 Channel
- **T1566.001** — Spearphishing Attachment

- **T1059.007** — JavaScript
- **T1105** — Ingress Tool Transfer
- **T1071.001** — Web Protocols
- **T1053.005** — Scheduled Task
- **T1056.001** — Keylogging
- **T1125** — Video Capture
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1113** — Screen Capture
- **T1218.005** — Mshta
- **T1027** — Obfuscated Files or Information
- **T1204.002** — Malicious File
- **T1059.003** — Windows Command Shell

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1036.004	Masquerade Task or Service	Defense-Evasion
T1608.004	Drive-by Target	Resource-Development
T1115	Clipboard Data	Collection
T1574.002	DLL Side-Loading	Persistence
T1090.001	Internal Proxy	Command-And-Control
T1083	File and Directory Discovery	Discovery
T1057	Process Discovery	Discovery
T1041	Exfiltration Over C2 Channel	Exfiltration
T1566.001	Spearphishing Attachment	Initial-Access
T1059.007	JavaScript	Execution
T1105	Ingress Tool Transfer	Command-And-Control
T1071.001	Web Protocols	Command-And-Control
T1053.005	Scheduled Task	Execution
T1056.001	Keylogging	Collection
T1125	Video Capture	Collection
T1547.001	Registry Run Keys / Startup Folder	Persistence
T1113	Screen Capture	Collection
T1218.005	Mshta	Defense-Evasion
T1027	Obfuscated Files or Information	Defense-Evasion
T1204.002	Malicious File	Execution
T1059.003	Windows Command Shell	Execution

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/pakistan-linked-sidecopy-targets....	T3

Source	URL	Tier
APT36 : Multi-Stage LNK Malware Campaign Targeting Indian ...	https://www.cyfirma.com/research/apt36-multi-stage-lnk-malware-camp...	T3
Stealth Fix: Microsoft Patches Exploited LNK Security Hole | SecPod	https://www.secpod.com/blog/stealth-fix-microsoft-patches-exploited...	T3
Pakistani group abuses Linux .desktop files for espionage - LinkedIn	https://www.linkedin.com/posts/rohit-dongre-x_linuxmalware-cybersec...	T3
APT36 LNK Phishing Uses mshta.exe to Deploy Fileless RAT	https://socprime.com/active-threats/apt36-multi-stage-lnk-malware-c...	T3

Generated 2026-06-02 14:02 UTC by TJS Security Command Center