INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 14:10 UTC

Pakistan-Linked Threat Actor Deploys Xeno RAT Against Afghan Finance Ministry in Targeted Espionage Campaign

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0407
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Afghan Finance Ministry systems; Xeno RAT v1.8.7 implant; DeskRAT; Golang ELF implant
Published	2026-06-04T00:01:00
Discovery Source	Rss

Executive Summary

Pakistan-linked threat group SideCopy (overlapping with APT36) has conducted a targeted espionage campaign, Operation XENOFISCAL, against Afghanistan's Ministry of Finance using the open-source Xeno RAT v1.8.7 implant alongside DeskRAT and a Golang ELF implant. The operation targets financial intelligence from a geopolitically significant government institution, exploiting documented capacity gaps rather than novel vulnerabilities. Organizations tracking South Asian threat actors, operating in the region, or sharing intelligence infrastructure with Afghan government counterparts face elevated risk of related activity.

Technical Analysis

SideCopy, a Pakistan-state-aligned threat actor with documented overlap with APT36, deployed Xeno RAT v1.8.7 (open-source RAT hosted on GitHub) as the primary implant in Operation XENOFISCAL, targeting the Afghan Ministry of Finance. Secondary tooling includes DeskRAT and a Golang-compiled ELF binary targeting Linux infrastructure. Attack chain relies on MITRE techniques: T1566 (phishing initial access), T1036 (masquerading), T1059 (command and script interpreter execution), T1105 (ingress tool transfer), T1547 (boot/logon autostart persistence), T1056.001 (keylogging), T1113 (screen capture), T1027 (obfuscated files), T1041 (exfiltration over C2 channel), T1071 (application layer protocol C2), and T1219 (remote access software). Applicable weaknesses are CWE-494 (Download of Code Without Integrity Check), relevant to Xeno RAT delivery via open-source repositories without integrity verification, and CWE-284 (Improper Access Control), relevant to persistence and lateral movement. No CVE is assigned; no vendor patch is applicable

given commodity and open-source tooling. Attribution confidence is assessed as moderate; use of open-source tooling is consistent with SideCopy's documented operational tradecraft to complicate attribution. No CISA KEV entry exists for this campaign.

Action Checklist

1. Containment, Block known Xeno RAT C2 communication patterns at the perimeter: inspect outbound traffic for application-layer protocol tunneling consistent with T1071; isolate any host exhibiting unexpected outbound connections to unfamiliar endpoints, particularly on non-standard ports. Apply NIST AC-4 (Information Flow Enforcement) to restrict unauthorized cross-boundary data flows.
2. Detection, Hunt for Xeno RAT v1.8.7 artifacts: search endpoint logs for process creation events spawning from user-writable directories, unexpected Golang ELF binaries on Linux hosts, and autostart registry or init configuration modifications (T1547, T1059). Review system init configurations per documented baselines. Query EDR/AV telemetry for unsigned binaries delivered via web or email. Enable CIS 8.2 (Collect Audit Logs) across all endpoints if not already active, and review AU-6 (Audit Record Review, Analysis, and Reporting) cadence.
3. Eradication, Remove identified Xeno RAT, DeskRAT, and Golang ELF implant artifacts from affected hosts. Audit autostart locations (registry run keys, scheduled tasks, Linux init configs) for persistence entries created by T1547. Revoke and rotate any credentials exposed to keylogging (T1056.001) per documented credential management procedures. Apply AC-6 (Least Privilege) to restrict accounts involved in impacted systems. Apply principle of least privilege to remove unnecessary access.
4. Recovery, Validate clean state of affected systems against known-good baselines using file integrity monitoring. Re-enable logging per AU-2 (Event Logging) and AU-12 (Audit Record Generation) and confirm log integrity per AU-9 (Protection of Audit Information). Monitor for re-infection indicators for a minimum of 30 days post-remediation, focusing on C2 beacon patterns (T1041, T1071) and reappearance of obfuscated files (T1027).
5. Post-Incident, Assess gaps in software integrity verification controls mapped to CWE-494: implement verification processes for any open-source or third-party tooling introduced to the environment, consistent with NIST CM controls. Conduct phishing simulation exercises targeting T1566 delivery vectors. Evaluate MFA coverage across externally exposed and administrative accounts per CIS 6.3, CIS 6.4, and CIS 6.5 to reduce initial access risk. Document lessons learned against NIST IR controls for future response playbook refinement.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior leadership and national CERT/CSIRT if evidence of successful data exfiltration from financial intelligence systems is confirmed, if any lateral movement beyond initially identified hosts is detected, or if the 2-person response team lacks capability to perform live memory forensics or malware reverse engineering required to fully characterize Xeno RAT v1.8.7 implant behavior in this environment.

Recovery Notes	Rebuild compromised hosts from verified clean images rather than attempting in-place remediation where feasible, given SideCopy/APT36's documented use of multiple overlapping implants (Xeno RAT, DeskRAT, Golang ELF) that may share persistence mechanisms — eradicating one without the others risks incomplete remediation. Monitor network egress for 30 days minimum post-remediation using a watchlist of all C2 indicators identified during the investigation, with particular attention to Xeno RAT's application-layer tunneling patterns on non-standard ports (T1071). Treat all credentials entered on any confirmed or suspected compromised host as fully rotated before restoring system access, given Xeno RAT v1.8.7's native keylogging capability (T1056.001) targeting financial system access credentials consistent with the campaign's intelligence collection objective.
Forensic Artifacts	Xeno RAT v1.8.7 binary and any associated DLL files in user-writable staging directories (%APPDATA%, %TEMP%, %PUBLIC% on Windows) — hash and preserve before removal; check for version-specific strings referencing the open-source GitHub repository origin that would confirm this specific implant variant | Keylogger output files written to disk by Xeno RAT's T1056.001 module — typically flat text or binary log files in the implant's working directory capturing financial system credentials, search for recently modified .log or .dat files under the implant staging path | Windows Registry autorun keys (HKCU\Software\Microsoft\Windows\CurrentVersion\Run and HKLM equivalent) and Windows Task Scheduler XML definitions containing paths to Xeno RAT or DeskRAT binaries, with creation timestamps correlating to the estimated intrusion window | Golang ELF binary artifacts on Linux hosts — preserve binary with full metadata (inode timestamps, file permissions, owning user) and extract import table and embedded strings using `strings` and `readelf -d` to confirm Golang runtime origin and identify C2 configuration compiled into the binary | Network PCAP or proxy/firewall logs showing outbound TCP sessions from affected hosts to non-inventoried external IPs on non-standard ports during the campaign window — Xeno RAT's C2 beaconing pattern (T1071 application-layer tunneling) will appear as periodic, low-volume outbound sessions with consistent jitter intervals characteristic of RAT beacon timing

Per-Action IR Details

Containment — Block known Xeno RAT C2 communication patterns at the perimeter: inspect outbound traffic for application-layer protocol tunneling consistent with T1071; isolate any host exhibiting unexpected outbound connections to unfamiliar endpoints, particularly on non-standard ports. Apply NIST AC-4 (Information Flow Enforcement) to restrict unauthorized cross-boundary data flows.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement)

Compensating: Use Wireshark or tcpdump on the network egress point to capture outbound traffic; filter for connections to IPs/domains not in your approved inventory using: `tcpdump -i eth0 'not net ' -w xeno_capture.pcap`. Parse PCAP with tshark filtering for non-standard port usage: `tshark -r xeno_capture.pcap -Y 'tcp.port != 80 && tcp.port != 443 && tcp.port != 53'`. Xeno RAT v1.8.7 supports custom C2 port configuration, so focus on stateful outbound TCP sessions on ports outside your approved egress baseline. Block at the host firewall using Windows Firewall netsh rules or iptables on Linux hosts pending full isolation.

Evidence: Before isolating, capture a full memory image of the suspect host using WinPmem (Windows) or LiME kernel module (Linux) to preserve in-memory Xeno RAT v1.8.7 process state, injected shellcode, and decrypted C2 configuration. Pull active network connection state with `netstat -anob` (Windows) or `ss -tulpn` (Linux) and record all ESTABLISHED and TIME_WAIT foreign addresses. Export DNS cache (`ipconfig /displaydns` or `/etc/hosts` review) to identify C2 hostname resolution artifacts. Capture firewall and proxy logs covering the 72-hour window prior to detection for outbound sessions initiated by the implant process.

Detection — Hunt for Xeno RAT v1.8.7 artifacts: search endpoint logs for process creation events spawning from user-writable directories, unexpected Golang ELF binaries on Linux hosts, and autostart registry or init configuration modifications (T1547, T1059). Review system init configurations per D3-SICA. Query EDR/AV telemetry for unsigned binaries delivered via web or email. Enable CIS 8.2 (Collect Audit Logs) across all endpoints if not already active, and review AU-6 (Audit Record Review, Analysis, and Reporting) cadence.

NIST Phase: Detection Analysis

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

Controls: CIS 8.2 (Collect Audit Logs), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: Deploy Sysmon with a hardened config (SwiftOnSecurity or olafhartong/sysmon-modular) and enable Event ID 1 (Process Create), Event ID 11 (File Create), and Event ID 3 (Network Connect). Hunt process creation from user-writable paths with PowerShell: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -match 'C:\\Users|AppData|Temp'}`. On Linux hosts, use `find / -type f -name '*.elf' -newer /var/log/auth.log 2>/dev/null` to surface recently dropped Golang ELF binaries. Use osquery with query `SELECT name, path, pid FROM processes WHERE path LIKE '%AppData%' OR path LIKE '%Temp%'` to enumerate suspicious process origins. Write a YARA rule targeting Xeno RAT v1.8.7 string artifacts (e.g., known GitHub repo strings, mutex names) and scan with: `yara -r xenorat.yar /path/to/scan`.

Evidence: Query Windows Security Event Log for Event ID 4688 (Process Creation) filtering on processes with parent paths in %APPDATA%, %TEMP%, or %PUBLIC% directories — Xeno RAT typically stages from user-writable locations to evade program-file integrity checks. On Linux, review `/var/log/syslog` and `/var/log/auth.log` for unexpected ELF execution events and check crontab entries (`crontab -l -u <user>`) and systemd unit files in `~/.config/systemd/user/` for SideCopy-planted persistence. Review Windows registry autorun keys: `HKCU\Software\Microsoft\Windows\CurrentVersion\Run` and `HKLM\Software\Microsoft\Windows\CurrentVersion\Run` for entries referencing non-standard binary paths consistent with DeskRAT or Xeno RAT staging. Check email gateway and proxy logs for delivery of archive files (ZIP, RAR) or document lures referencing Afghan Finance Ministry themes, consistent with SideCopy/APT36 T1566 spearphishing tradecraft.

Eradication — Remove identified Xeno RAT, DeskRAT, and Golang ELF implant artifacts from affected hosts. Audit autostart locations (registry run keys, scheduled tasks, Linux init configs) for persistence entries created by T1547. Revoke and rotate any credentials exposed to keylogging (T1056.001) per D3-CRO (Credential Rotation). Apply AC-6 (Least Privilege) to restrict accounts involved in impacted systems. Apply D3-UAP (User Account Permissions) to remove unnecessary access.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege)

Compensating: Enumerate and remove all scheduled tasks created after the estimated compromise date using: `schtasks /query /fo LIST /v | findstr /i 'Task Name\|Status\|Run As\|Task To Run'` and delete suspicious entries with `schtasks /delete /tn "<taskname>" /f`. For Linux, audit all crontabs (`for user in $(cut -f1 -d: /etc/passwd); do crontab -u $user -l 2>/dev/null; done`) and remove SideCopy-planted entries. Delete Golang ELF binaries identified during detection phase; verify removal with `md5sum` against known-good file hashes. Force-rotate all credentials for accounts active on compromised hosts using Active Directory `Set-ADAccountPassword` or local `net user <username>`. For keylogger exposure (T1056.001 via Xeno RAT's built-in keylog module), treat all credentials entered on affected hosts as fully compromised — this includes financial system credentials relevant to the Afghan Finance Ministry targeting.

Evidence: Before removing implant files, collect and preserve: full filesystem timeline from affected hosts using `fls` (Sleuth Kit) or `MFTECmd` to document Xeno RAT, DeskRAT, and Golang ELF binary creation timestamps and parent directory context. Export complete registry hive copies (SYSTEM, SOFTWARE, NTUSER.DAT) from affected Windows hosts prior to eradication to preserve forensic record of T1547 autostart entries. Capture keylogger output files if present — Xeno RAT v1.8.7 stores keylog data locally before exfil; search for `.log` or `.dat` files in staging directories under %APPDATA% or %TEMP%. Document all scheduled task XML definitions and Linux init configs in their pre-removal state for post-incident analysis.

Recovery — Validate clean state of affected systems against known-good baselines using D3-SFA (System File Analysis). Re-enable logging per AU-2 (Event Logging) and AU-12 (Audit Record Generation) and confirm log integrity per AU-9 (Protection of Audit Information). Monitor for re-infection indicators for a minimum of 30 days post-remediation, focusing on C2 beacon patterns (T1041, T1071) and reappearance of obfuscated files (T1027).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-2 (Event Logging), NIST AU-9 (Protection Of Audit Information), NIST AU-12 (Audit Record Generation)

Compensating: Validate system file integrity against known-good baselines using Windows SFC (`sfc /scannow`) and DISM (`DISM /Online /Cleanup-Image /RestoreHealth`) for Windows hosts; use `rpm -Va` or `debsums -c` on Linux hosts to detect tampered system binaries. For ongoing beacon detection without SIEM, configure Sysmon Event ID 3 (Network Connect) with a 30-day watchlist of previously identified SideCopy C2 indicators and pipe alerts to a local log file reviewed daily. Use ClamAV with a custom signature database updated with Xeno RAT v1.8.7 YARA rules for recurring scans: `clamscan -r --infected /path/to/scan`. Forward Sysmon and Windows Event Logs to a centralized syslog server (even a local rsyslog instance) to protect log integrity against tampering by any residual implant activity, satisfying AU-9 intent without enterprise SIEM.

Evidence: Prior to returning systems to production, document: verified hash comparison results for all system binaries against vendor-provided or pre-compromise baselines, confirming no Xeno RAT or DeskRAT remnants. Confirm log continuity — check for gaps in Windows Security Event Log or Linux syslog timestamps that could indicate SideCopy's use of log tampering or implant-driven log suppression. Capture a post-remediation memory image to confirm no residual in-memory implant presence before declaring the host clean. Retain all forensic images, captured PCAPs, and artifact collections under chain-of-custody for a minimum of 90 days given the state-linked (Pakistan/SideCopy-APT36) attribution and potential intelligence or legal value.

Post-Incident — Assess gaps in software integrity verification controls mapped to CWE-494: implement verification processes for any open-source or third-party tooling introduced to the environment, consistent with NIST CM controls. Conduct phishing simulation exercises targeting T1566 delivery vectors. Evaluate MFA coverage across externally exposed and administrative accounts per CIS 6.3, CIS 6.4, and CIS 6.5 to reduce initial access risk. Document lessons learned against NIST IR controls for future response playbook refinement.

NIST Phase: Post Incident

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

Controls: CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For CWE-494 (Download of Code Without Integrity Check) remediation without enterprise tooling: implement a mandatory SHA-256 hash verification step (documented in a one-page SOP) for all open-source tools introduced to the environment, comparing against upstream publisher hashes — Xeno RAT was sourced from a public GitHub repository and could have been trojanized at the acquisition stage. For phishing simulation targeting SideCopy/APT36 T1566 lure themes (geopolitical documents, Finance Ministry-themed decoys), use the free GoPhish framework to run internal exercises. For MFA gap assessment, enumerate accounts without MFA using `Get-MsolUser -All | Where-Object {$_.StrongAuthenticationMethods.Count -eq 0}` (Azure AD) or equivalent on-premise tooling and prioritize accounts with access to financial systems matching the campaign's targeting profile.

Evidence: Compile a post-incident lessons-learned package including: timeline reconstruction of SideCopy's initial access vector (spearphish, watering hole, or supply chain — specific to the Afghan Finance Ministry targeting), dwell time from estimated initial compromise to detection, all identified persistence mechanisms (T1547 autostart entries, scheduled tasks, Linux init configs) with timestamps, and a full inventory of credentials and data categories potentially exfiltrated via Xeno RAT's keylog and file collection modules. This package directly informs playbook updates for future SideCopy/APT36 campaigns targeting South Asian government financial institutions.

Detection Guidance

Hunt for Xeno RAT v1.8.7 indicators using the following approach: (1) EDR/AV: search for unsigned PE or ELF binaries executing from user-writable paths (temp directories, AppData, /tmp); flag Golang-compiled ELF binaries on Linux hosts where none are expected. (2) Network: inspect outbound connections for periodic beaconing patterns consistent with T1071 application-layer C2; look for HTTP/S traffic to recently registered or low-reputation domains with abnormal user-agent strings. (3) Endpoint logs: alert on autostart persistence modifications (Windows registry run keys, Linux init/systemd configs) correlating with T1547; monitor for keylogging-associated API calls (T1056.001) and screen capture activity (T1113). (4) Phishing delivery (T1566): review email gateway logs for documents with embedded macros or links delivering executables; correlate with T1105 ingress tool transfer events. (5) File integrity: apply file magic byte verification to flag files whose extension does not match their magic bytes, a common masquerading indicator (T1036). (6) Audit local accounts for unexpected creation or privilege changes per account monitoring procedures. Source URLs provided in this item are T3 (news-tier); IOC lists should be cross-referenced against primary threat intelligence platforms before operationalizing.

Indicators of Compromise

Type	Value	Context	Confidence
HASH	`not confirmed in available T3 sources`	Xeno RAT v1.8.7 binary hash — not confirmed in available T3 sources; obtain from primary threat intelligence feed before operationalizing	LOW
HASH	`not confirmed in available T3 sources`	DeskRAT binary hash — not confirmed in available T3 sources	LOW
HASH	`not confirmed in available T3 sources`	Golang ELF implant hash — not confirmed in available T3 sources	LOW

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1036** — Masquerading
- **T1056.001** — Keylogging
- **T1105** — Ingress Tool Transfer
- **T1547** — Boot or Logon Autostart Execution
- **T1041** — Exfiltration Over C2 Channel
- **T1113** — Screen Capture
- **T1059** — Command and Scripting Interpreter
- **T1027** — Obfuscated Files or Information
- **T1219** — Remote Access Tools

- **T1071** — Application Layer Protocol

NIST-800-53R5

- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CM-7** — Least Functionality
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control
- **AC-3** — Access Enforcement
- **IR-5** — Incident Monitoring

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures
- **A01:2021** — Broken Access Control

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored
- **DE.AE-08** — Incidents are declared when adverse events meet the defined incident criteria

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1036	Masquerading	Defense-Evasion

Technique ID	Technique Name	Tactic
T1056.001	Keylogging	Collection
T1105	Ingress Tool Transfer	Command-And-Control
T1547	Boot or Logon Autostart Execution	Persistence
T1041	Exfiltration Over C2 Channel	Exfiltration
T1113	Screen Capture	Collection
T1059	Command and Scripting Interpreter	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1219	Remote Access Tools	Command-And-Control
T1071	Application Layer Protocol	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/pakistan-spi...	T3
Pakistan-Linked SideCopy Targets Afghanistan Finance Ministry ...	https://thehackernews.com/2026/06/pakistan-linked-sidecopy-targets....	T3
The Hacker News - Facebook	https://www.facebook.com/thehackernews/posts/%EF%B8%8F-pakistan-ali...	T3
SideCopy/APT36 Operation XENOFISCAL: Xeno RAT 1.8.7 Targets	https://techjacksolutions.com/scc-intel/sidecopy-apt36-operation-xe...	T3
SideCopy group targets Afghanistan's Ministry of Finance with Xeno ...	https://www.scworld.com/brief/sidecopy-group-targets-afghanistans-m...	T3

Generated 2026-06-04 14:10 UTC by TJS Security Command Center