INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-19 13:49 UTC

LatAm Threat Actor Blends Opportunistic Monetization with Intelligence Collection in Hybrid Operation

THREAT CAMPAIGN | **HIGH** | CVSS 5.0

SCC Item ID	SCC-CAM-2026-0518
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	5.0
Affected Products	Not specified, regional targeting across Latin America; specific products/sectors not identified in available source material
Published	2026-06-18T15:09:21
Discovery Source	Rss

Executive Summary

A threat group designated 'Operation Escaneo' is running hybrid operations across Latin America, combining financially motivated cybercrime with apparent intelligence collection against regional targets. The dual-objective structure, possibly funded by criminal revenues to support espionage activity, represents a notable operational model. Organizations with operations, partners, or supply chain exposure in Latin America face elevated risk from both data theft and financial fraud vectors simultaneously.

Technical Analysis

Operation Escaneo is a hybrid campaign attributed to an untracked threat group operating across Latin America. No CVE or specific product vulnerability anchors this campaign; initial access is inferred to involve phishing (T1566, confidence LOW) and valid account abuse (T1078). Post-compromise activity includes file and directory enumeration (T1083), automated collection (T1119), masquerading (T1036), and data exfiltration over C2 channels (T1041). The ransomware or extortion component maps to T1486 (Data Encrypted for Impact). Infrastructure acquisition (T1583) is inferred at LOW confidence, suggesting possible shared or brokered infrastructure across multiple operators. The campaign structure, dual financial and intelligence objectives with apparent low operational coordination between them, is consistent with either a multi-operator model or a principal-agent arrangement where criminal monetization subsidizes intelligence tasking. CVSS does not apply to campaign-type items; severity is qualitative. Source: single T3 article (Dark Reading); no primary-tier corroboration from CISA, MITRE, or NVD. All TTP attributions and actor characterizations carry LOW

confidence pending additional reporting.

Action Checklist

1. Step 1: Containment. Audit accounts with access to regionally exposed systems or Latin America-facing infrastructure. Disable or isolate accounts showing anomalous access patterns. Apply CIS Controls v8 5.3 (Disable Dormant Accounts) and CIS Controls v8 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) to reduce standing access. Confidence in specific IOCs is LOW; cast a wide net on behavioral anomalies.
2. Step 2: Detection. Review logs for enumeration activity (T1083: unusual directory traversal, file listing commands), bulk data staging (T1119: large file copies to temp directories), and outbound C2 traffic (T1041: sustained beaconing to non-baseline external IPs). Per NIST AU-6, conduct targeted review of audit records for these behavioral patterns across endpoints and servers with LatAm-region exposure. No confirmed IOC hashes, IPs, or domains are available in source material.
3. Step 3: Eradication. There is no patch to apply; this campaign exploits valid credentials and user behavior, not a named vulnerability. Rotate credentials for any accounts active on affected or regionally exposed systems per NIST AC-2 (Account Management). Enforce MFA on all externally exposed applications per CIS Controls v8 6.3 and CIS Controls v8 6.4. Review and remove unauthorized or unrecognized accounts per NIST AC-2.
4. Step 4: Recovery. Validate that MFA enforcement is active on all externally exposed and administrative accounts. Confirm outbound C2 channels are blocked via firewall policy per CIS Controls v8 4.4 and CIS Controls v8 4.5. Monitor for re-access attempts using previously compromised credentials. Ensure audit logging is active and retention meets policy per NIST AU-11 and CIS Controls v8 8.2.
5. Step 5: Post-Incident. This campaign exposes gaps in behavioral detection for hybrid threat actors who blend financially motivated and espionage-oriented activity. Review detection rules for enumeration, bulk collection, and exfiltration chains. Assess whether your threat intelligence program covers LatAm regional actors. Map control gaps against NIST AC-6 (Least Privilege) and AU-6 (Audit Record Review) as foundational improvements.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to senior leadership, legal, and external IR retainer if behavioral analysis confirms exfiltration of customer PII, financial records, or strategic business data from LatAm-exposed systems, as this may trigger breach notification obligations under applicable regional privacy regulations (e.g., Brazil LGPD, Argentina PDPA) or activate cyber insurance coverage conditions; also escalate if evidence suggests the intelligence-collection objective is targeting your organization's strategic plans, M&A activity, or government-adjacent operations.

Recovery Notes	Recovery validation for Operation Escaneo must focus on credential hygiene and access channel integrity rather than patch verification, since this campaign abuses valid credentials and legitimate tooling rather than exploiting a named vulnerability. Monitor authentication logs for Event ID 4624 and 4648 filtered on all accounts that were active on LatAm-exposed systems during the incident window for a minimum of 30 days post-rotation, as threat actors in hybrid campaigns frequently retain backup credential sets or re-establish access through supply chain or partner channels. Confirm that behavioral detection rules for enumeration-staging-exfiltration chains authored in Step 5 are generating test alerts as expected before closing the incident, and schedule a 30-day and 90-day reassessment to verify no re-intrusion has occurred.
Forensic Artifacts	Windows Security Event Log entries for Event ID 4624 (logon), 4648 (explicit credential use), and 4672 (special privilege logon) on all systems with LatAm-region remote access, filtered to the incident timeframe — these are the primary authentication trail for credential-abuse operations like Operation Escaneo | Sysmon Event ID 1 (process creation) logs capturing cmd.exe, powershell.exe, wscript.exe, and cscript.exe invocations with parent process context, specifically where parent is a remote-access or web-facing service — consistent with the enumeration and staging TTPs attributed to this campaign | Contents of `C:\Users\*\AppData\Local\Temp\`, `C:\Windows\Temp\`, and any mapped network share temp directories for staged archive files (ZIP, RAR, 7z) or reconnaissance output files (CSV, TXT) created during the incident window — bulk staging to temp directories is a behavioral signature of the data collection phase of this campaign | Scheduled task XML exports (`C:\Windows\System32\Tasks\`) and registry run key snapshots (`HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`) timestamped to the incident window — hybrid actors like Operation Escaneo establishing persistent footholds for intelligence collection commonly leverage these mechanisms | Outbound NetFlow or perimeter firewall connection logs filtered on sustained low-frequency connection intervals (beaconing pattern) to non-baseline external IPs, particularly connections originating from endpoints or servers with LatAm-region access roles — the C2 infrastructure for this campaign is not publicly identified, making behavioral beaconing pattern analysis the primary network-layer indicator

Per-Action IR Details

Step 1: Containment — Audit accounts with access to regionally exposed systems or Latin America-facing infrastructure. Disable or isolate accounts showing anomalous access patterns. Apply CIS 5.3 (Disable Dormant Accounts) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) to reduce standing access. Confidence in specific IOCs is LOW; cast a wide net on behavioral anomalies.

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Export Active Directory last-logon data with PowerShell: `Get-ADUser -Filter * -Properties LastLogonDate | Where-Object { $_.LastLogonDate -lt (Get-Date).AddDays(-45) } | Select-Object Name,SamAccountName,LastLogonDate | Export-Csv dormant_accounts.csv`. For Linux, parse `/var/log/lastlog` with `lastlog | grep -v 'Never'`. Disable accounts manually after review. A 2-person team can divide by region: one audits privileged accounts, one audits service/shared accounts touching LatAm-exposed systems.

Evidence: Before disabling or isolating any account, capture the live authentication state: export current active session tokens and Kerberos ticket cache (`klist` on Windows endpoints; `klist -l` for all sessions). Pull Windows Security Event Log Event ID 4624 (successful logon), 4625 (failed logon), and 4648 (explicit credential use) filtered to accounts with

LatAm-region VPN or remote access entries for the prior 30 days. On Linux systems, collect `/var/log/auth.log` and `/var/log/secure` before account lockout. Capture `net session` and `quser` output on Windows servers to enumerate live sessions from regionally sourced IPs prior to any account disable action.

Step 2: Detection — Review logs for enumeration activity (T1083: unusual directory traversal, file listing commands), bulk data staging (T1119: large file copies to temp directories), and outbound C2 traffic (T1041: sustained beaconing to non-baseline external IPs). Per NIST AU-6, conduct targeted review of audit records for these behavioral patterns across endpoints and servers with LatAm-region exposure. No confirmed IOC hashes, IPs, or domains are available in source material.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation)

Compensating: Deploy Sysmon with SwiftOnSecurity config to capture Event ID 1 (process creation) and Event ID 3 (network connections). Hunt enumeration with: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Id -eq 1 -and $_.Message -match 'cmd.exe|dir |tree |robocopy|xcopy'}`. For C2 beaconing detection without a SIEM, use Wireshark with display filter `tcp.flags.syn==1 && ip.dst != ` and sort by destination IP frequency over a 24-hour pcap. Use the free Sigma rule 'Bulk File Copy to Temp Directory' (rule ID proc_creation_win_robocopy_lolbin.yml) converted to a PowerShell query against Sysmon logs.

Evidence: This step is analytical and does not alter live state; however, capture the following before any follow-on containment actions that may flush logs: export Sysmon Event ID 1 logs filtered on `cmd.exe`, `powershell.exe`, `wscript.exe`, and `cscript.exe` spawned from non-interactive parent processes — consistent with the credential-abuse pattern seen in Operation Escaneo. Collect Windows Prefetch files from `C:\Windows\Prefetch\` for staging tools (robocopy, xcopy, 7zip, rar). Pull outbound NetFlow or firewall connection logs filtered on connections to non-baseline IPs, especially sustained low-frequency (beaconing) intervals of 30–300 seconds to LatAm or anonymizing-infrastructure destinations. Capture `C:\Users\*\AppData\Local\Temp\` directory listings on endpoints with LatAm-region access before any cleanup.

Step 3: Eradication — There is no patch to apply; this campaign exploits valid credentials and user behavior, not a named vulnerability. Rotate credentials for any accounts active on affected or regionally exposed systems per D3-CRO (Credential Rotation). Enforce MFA on all externally exposed applications per CIS 6.3 and CIS 6.4. Review and remove unauthorized or unrecognized accounts per NIST AC-2.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery

Controls: NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: For credential rotation without an enterprise PAM tool, use PowerShell to force password reset across all accounts active on LatAm-exposed systems: `Set-ADUser -Identity -ChangePasswordAtLogon $true`. For MFA enforcement on externally exposed apps without an enterprise IdP, enable Windows Hello for Business or deploy the free tier of Duo Security (up to 10 users) for VPN and RDP gateways. Document each rotated account and timestamp in a shared incident log so the 2-person team maintains a synchronized state.

Evidence: Before rotating any credentials, capture the full credential state to preserve forensic timeline: run `net user /domain` and export all account attributes including password last set, last logon, and group membership to a timestamped CSV. On systems where Operation Escaneo actors may have established persistence via scheduled tasks or registry run keys, collect `schtasks /query /fo LIST /v > scheduled_tasks_pre_rotation.txt` and export `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` and `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` before any account or system changes. Capture active NTLM and Kerberos sessions (`klist purge` output deferred until after capture) to document which credentials were in active use at time of rotation.

Step 4: Recovery — Validate that MFA enforcement is active on all externally exposed and administrative accounts. Confirm outbound C2 channels are blocked via firewall policy per CIS 4.4 and CIS 4.5. Monitor for re-access attempts using previously compromised credentials. Ensure audit logging is active and retention meets policy per NIST AU-11 and CIS 8.2.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-11 (Audit Record Retention), NIST AU-2 (Event Logging), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 8.2 (Collect Audit Logs)

Compensating: Validate host-based firewall egress rules on servers using `netsh advfirewall show allprofiles` (Windows) or `iptables -L OUTPUT -n -v` (Linux); confirm no rules permit outbound to non-baseline external IPs on ports commonly used for C2 (e.g., 443, 80, 8080, 4444). For re-access monitoring without a SIEM, create a PowerShell scheduled task to run every 4 hours parsing Security Event Log for Event ID 4624 filtered on the previously compromised account SamAccountNames and alert via email if any match is found. Verify audit log retention policy with `auditpol /get /category:*` and confirm Windows Event Log max size is set to at least 1GB per critical log channel.

Evidence: This step validates recovery state rather than altering active compromise artifacts; however, before confirming recovery, verify that no new scheduled tasks, services, or registry persistence keys were created during the incident window. Run `Get-ScheduledTask | Where-Object {$_.Date -gt ''}` and compare against the pre-rotation baseline captured in Step 3. Collect a final snapshot of outbound firewall logs to confirm C2 beaconing intervals have ceased — absence of the sustained low-frequency connection pattern identified in Step 2 is the primary recovery indicator for this campaign's C2 behavior.

Step 5: Post-Incident — This campaign exposes gaps in behavioral detection for hybrid threat actors who blend financially motivated and espionage-oriented activity. Review detection rules for enumeration, bulk collection, and exfiltration chains. Assess whether your threat intelligence program covers LatAm regional actors. Map control gaps against NIST AC-6 (Least Privilege) and AU-6 (Audit Record Review) as foundational improvements.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Author or adapt Sigma detection rules targeting the three behavioral chains observed in Operation Escaneo: (1) directory enumeration via cmd.exe/PowerShell spawned from web-facing or remote-access processes, (2) bulk file copy to `%TEMP%` or `%APPDATA%` directories, and (3) sustained outbound connections at regular intervals to IPs not in your network baseline. Publish rules to your Sysmon pipeline using `sigmac -t powershell`. For LatAm threat intelligence coverage without a commercial TI subscription, monitor CISA alerts, MITRE ATT&CK Groups page for LatAm-attributed actors, and regional CSIRTs (e.g., LACNIC's security working group) as free sources. Document lessons learned in a structured after-action report referencing this campaign's hybrid monetization-plus-espionage model as a threat archetype for future tabletop exercises.

Evidence: Preserve the complete incident artifact package for the lessons-learned review: the timestamped account audit CSV from Step 3, Sysmon event exports from Step 2, firewall log snapshots from Step 4, and the scheduled task baseline comparison from Step 4. This evidence set should be stored in write-once or access-controlled storage per NIST AU-9 (Protection of Audit Information) and retained for a minimum period consistent with your organization's incident record retention policy. The hybrid nature of Operation Escaneo — financial crime funding intelligence collection — means the same artifact set may be relevant to both a fraud investigation and a counterintelligence review, so chain-of-custody documentation is particularly important.

Detection Guidance

No confirmed IOCs (IPs, domains, hashes) are available in source material at this time; the following guidance is based on mapped MITRE techniques at LOW confidence. Monitor for: (1) T1083, unusual file and directory enumeration via command-line tools or scripting engines on endpoints; (2) T1119, automated file collection to staging directories, particularly large or recursive copy operations; (3) T1041, sustained outbound connections to non-baseline external IPs, especially over common ports (80, 443) with unusual data volumes; (4) T1078, logons from unfamiliar geolocations or outside business hours using valid credentials; (5) T1036, processes with names mimicking legitimate system binaries running from unexpected paths. Per NIST AU-6, establish a regular review cadence for these behavioral patterns. Use NIST AC-2 (Account Management) to flag anomalous local account activity. SIEM correlation rules should chain enumeration, staging, and exfiltration events rather than alerting on each in isolation. Confidence in all detection guidance is LOW pending corroborating primary-tier reporting.

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1583** — Acquire Infrastructure
- **T1083** — File and Directory Discovery
- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing
- **T1036** — Masquerading
- **T1078** — Valid Accounts
- **T1119** — Automated Collection

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1583	Acquire Infrastructure	Resource-Development
T1083	File and Directory Discovery	Discovery
T1486	Data Encrypted for Impact	Impact
T1566	Phishing	Initial-Access
T1036	Masquerading	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1119	Automated Collection	Collection

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cybersecurity-operations/operation-esca...	T3
Vulnerability In Apache Commons Text Library	https://northwave-cybersecurity.com/threat-response/vulnerability-i...	T3
Security Notice: Apache commons-text vulnerability (CVE-2022 ...	https://support.xmatters.com/hc/en-us/articles/13843436346139-Secur...	T3
Vulnerability (Text4Shell) (CVE-2022-42889) - Cloudera Community	https://community.cloudera.com/t5/Support-Questions/Vulnerability-T...	T3
Critical vulnerability surfaces in Apache Commons Text library	https://www.cybersecuritydive.com/news/critical-vulnerability-apach...	T3

Generated 2026-06-19 13:49 UTC by TJS Security Command Center