INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-04 06:48 UTC

Multi-Sector Data Breaches Claimed by TheGentlemen and Nova Threat Groups, June 2026

DATA BREACH | HIGH

SCC Item ID	SCC-DBR-2026-0146
Type	Data Breach
Severity	HIGH
Affected Products	Anandji Haridas & Co. Pvt. Ltd. (Manufacturing, India); Arabian Procession Holding (Investment); Indonesia's Badan Pangan Nasional (National Food Agency, Government)
Published	2026-06-02
Discovery Source	Gemini

Executive Summary

Three organizations across manufacturing, investment, and government sectors have been named in data breach claims by two threat groups, TheGentlemen and Nova, in early June 2026. The affected entities, an Indian manufacturing firm, a Middle Eastern investment holding company, and Indonesia's national food agency, span high-value industries where data theft can expose sensitive business, financial, and government operational information. Attribution confidence is low-to-medium; no technical exploitation details are confirmed, but the multi-sector targeting pattern is consistent with financially motivated or data-brokerage actors who sell exfiltrated data on criminal markets.

Technical Analysis

Breach claims attributed to TheGentlemen and Nova emerged in early June 2026 targeting Anandji Haridas & Co. Pvt. Ltd. (Indian manufacturing), Arabian Procession Holding (investment), and Indonesia's Badan Pangan Nasional (government food agency). No CVE identifiers, CWE classifications, or CVSS scores are associated with these incidents. MITRE ATT&CK techniques referenced in available metadata include T1566 (Phishing, initial access), T1078 (Valid Accounts, persistence and lateral movement), T1119 (Automated Collection), T1530 (Data from Cloud Storage), and T1041 (Exfiltration Over C2 Channel). These techniques collectively describe a plausible intrusion chain: phishing or credential theft for initial access, collection from cloud or internal storage, and exfiltration, but this chain is inferred from actor patterns, not confirmed forensic evidence. Data types exfiltrated, affected systems, and victim impact scope are unconfirmed. Source material derives from T3 sources (CybersecurityHunter.com, Breachsense); no primary vendor advisories or government disclosures are

available. Attribution to TheGentlemen and Nova is based on self-reported claims. Overall confidence: low-to-medium.

Action Checklist

1. Step 1: Containment. If your organization shares sector characteristics (manufacturing, investment, or government food/agriculture) with named victims, audit externally facing authentication surfaces immediately. Enforce NIST AC-17 (Remote Access) controls; verify that all remote access paths require MFA per CIS 6.4 and CIS 6.5. Disable or isolate any accounts showing anomalous login behavior per NIST AC-2 (Account Management).
2. Step 2: Detection. Review authentication logs for T1078 indicators: logins outside business hours, from unfamiliar geolocations, or using dormant accounts. Hunt for T1566 delivery artifacts in email gateway logs. Inspect cloud storage access logs (T1530) for bulk reads or exports by non-privileged accounts. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) cadence. Use NIST AC-2 (Account Management) monitoring to flag lateral movement via compromised local credentials.
3. Step 3: Eradication. Rotate credentials for any accounts that may have been exposed per NIST IA-4 (Identifier Management) and IA-5 (Authentication). Enforce unique, complex passwords per CIS 5.2. Disable dormant accounts per CIS 5.3 (threshold: 45 days inactivity). Review and restrict cloud storage permissions to least-privilege per NIST AC-6 and CIS 3.3 (Configure Data Access Control Lists). No specific patch exists; remediation centers on access hygiene.
4. Step 4: Recovery. Verify MFA enforcement across all external-facing applications (CIS 6.3) and administrative accounts (CIS 6.5). Confirm audit logging is active and forwarding to a protected SIEM per NIST AU-9 (Protection of Audit Information) and CIS 8.2 (Collect Audit Logs). Monitor post-remediation for re-authentication attempts using previously valid credentials. Apply NIST IA-5 (Authentication) controls enterprise-wide.
5. Step 5: Post-Incident. Assess control gaps in phishing prevention (T1566 mitigation) and cloud data governance (T1530). If no data inventory exists, establish one per CIS 3.2 (Establish and Maintain a Data Inventory). Conduct a review of third-party and external system access policies per NIST AC-20 (Use of External Systems). Document findings and update incident playbooks to address opportunistic, multi-sector breach campaigns.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if forensic review of cloud storage access logs confirms that sensitive business, financial, or government operational data was accessed or staged for exfiltration by compromised accounts, triggering mandatory breach notification obligations under India's DPDP Act, Indonesia's PDP Law, or applicable GCC data protection regulations within their prescribed notification windows.

Recovery Notes	Post-containment, maintain enhanced authentication monitoring for a minimum of 30 days, specifically watching for re-authentication attempts using credential patterns (usernames, email formats) associated with the breach window — opportunistic groups like TheGentlemen and Nova have demonstrated willingness to return to previously compromised organizations. Verify that all cloud storage permission changes made during eradication persist and have not been silently reverted by automated provisioning tools or IaC pipelines (Terraform, CloudFormation) that may re-apply pre-breach configurations. Confirm that data inventory (CIS 3.2) and third-party access reviews (NIST AC-20) initiated during post-incident are completed within 30 days and integrated into the updated incident playbook before closing the incident record.
Forensic Artifacts	Cloud IdP sign-in logs (Azure AD Sign-in logs / AWS CloudTrail ConsoleLogin / Google Workspace Admin Audit) for the 30-day pre-detection window — primary evidence of T1078 valid account abuse, showing source IPs, geolocations, user agents, and MFA bypass indicators specific to credential-based initial access used by TheGentlemen and Nova | Cloud storage access logs (AWS S3 Server Access Logs or CloudTrail Data Events, Azure Blob Storage diagnostic logs, SharePoint Unified Audit Log) filtered for bulk GetObject/download events by non-privileged or dormant accounts — directly maps to T1530 cloud data staging behavior claimed in these breach incidents | Email gateway message trace logs including full headers, sender IP, attachment file names and hashes, and click/delivery status for the 30-day pre-detection window — supports T1566 phishing delivery investigation for initial access into manufacturing and government sector targets with limited security tooling | Active Directory last-logon audit export and OAuth/API token inventory from cloud environments at time of discovery — establishes the scope of compromised credential exposure and identifies persisted access mechanisms (long-lived tokens, service accounts) that survive password resets | Windows Security Event Log entries: Event ID 4624 (Successful Logon), 4625 (Failed Logon), 4648 (Explicit Credential Use), and 4720 (User Account Created) from domain controllers and remote access gateway hosts — provides on-premises lateral movement evidence to correlate with cloud-side T1078 indicators in this multi-vector, credential-focused campaign

Per-Action IR Details

Step 1: Containment — If your organization shares sector characteristics (manufacturing, investment, or government food/agriculture) with named victims, audit externally facing authentication surfaces immediately. Enforce NIST AC-17 (Remote Access) controls; verify that all remote access paths require MFA per CIS 6.4 and CIS 6.5. Disable or isolate any accounts showing anomalous login behavior per NIST AC-2 (Account Management).

NIST Phase: Containment

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

Controls: NIST AC-2 (Account Management), NIST AC-17 (Remote Access), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Export active VPN/remote access session logs manually from your firewall or VPN concentrator (e.g., Fortinet: `get vpn ssl monitor`, Cisco ASA: `show vpn-sessiondb`). Cross-reference against an account inventory spreadsheet for accounts not seen in the past 45 days. For MFA gap identification without a commercial IAM tool, run `net user /domain` on Windows AD and flag accounts lacking a registered MFA device in your IdP's admin console (Duo, Azure AD free tier, or Google Workspace). Block flagged accounts with `Disable-ADAccount -Identity ` in PowerShell.

Evidence: Before disabling any accounts, capture a full export of currently active sessions from your VPN/remote access gateway (session logs, source IPs, timestamps, account names). Dump Active Directory last-logon timestamps

with `Get-ADUser -Filter * -Properties LastLogonDate | Export-CSV`. Preserve cloud IdP sign-in logs (Azure AD Sign-in logs, AWS CloudTrail `ConsoleLogin` events, or Google Workspace Admin audit logs) covering the prior 30 days — TheGentlemen and Nova campaigns targeting investment and government sectors have involved credential-based initial access, so these logs are your primary evidence of unauthorized entry prior to containment.

Step 2: Detection — Review authentication logs for T1078 indicators: logins outside business hours, from unfamiliar geolocations, or using dormant accounts. Hunt for T1566 delivery artifacts in email gateway logs. Inspect cloud storage access logs (T1530) for bulk reads or exports by non-privileged accounts. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) cadence. Use D3-LAM (Local Account Monitoring) to flag lateral movement via compromised local credentials.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-2 (Event Logging), NIST AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run targeted PowerShell against Windows Security Event Log: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.TimeCreated.Hour -notin 7..18}` to surface off-hours logins (T1078). For T1566, query your email gateway's message trace (Microsoft 365: `Get-MessageTrace` via Exchange Online PowerShell; Google Workspace: Admin console > Reports > Email Log Search) filtering on attachments with extensions .lnk, .iso, .html, .zip from external senders in the 30 days prior. For T1530 cloud storage exfiltration, query AWS CloudTrail for `GetObject` events by IAM users not in your admin group, or pull Google Drive audit logs filtering on `download` events by non-admin accounts exceeding 50 files in a single session. Use free Sigma rules mapped to T1078 and T1530 (available at github.com/SigmaHQ/sigma) converted to your query language with sigmac.

Evidence: Preserve email gateway logs including full message headers, sender IP, and attachment metadata for all inbound messages in the 30-day window preceding detection — T1566 phishing is a likely initial access vector for both TheGentlemen and Nova based on their claimed breach patterns against non-technical sector targets (manufacturing, government food agency). Capture cloud storage access logs (AWS S3 access logs, Azure Blob Storage diagnostic logs, or SharePoint Unified Audit Logs) with particular attention to bulk `GetObject`/download events, which would reflect T1530 data staging prior to exfiltration. Preserve Windows Security Event Log Event ID 4624 (Successful Logon) and 4648 (Explicit Credential Use) for all accounts, and Event ID 4625 (Failed Logon) to identify credential stuffing attempts consistent with opportunistic breach campaigns.

Step 3: Eradication — Rotate credentials for any accounts that may have been exposed (D3-CRO: Credential Rotation). Enforce unique, complex passwords per CIS 5.2. Disable dormant accounts per CIS 5.3 (threshold: 45 days inactivity). Review and restrict cloud storage permissions to least-privilege per NIST AC-6 and CIS 3.3 (Configure Data Access Control Lists). No specific patch exists; remediation centers on access hygiene.

NIST Phase: Eradication

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

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.2 (Use Unique Passwords), CIS 5.3 (Disable Dormant Accounts), CIS 3.3 (Configure Data Access Control Lists)

Compensating: Identify dormant accounts with `Get-ADUser -Filter {Enabled -eq $true} -Properties LastLogonDate | Where-Object {$_.LastLogonDate -lt (Get-Date).AddDays(-45)} | Select Name, LastLogonDate` and pipe to `Disable-ADAccount`. For cloud storage ACL review without a CSPM tool, use AWS CLI: `aws s3api get-bucket-acl --bucket ` and `aws iam get-account-authorization-details` to enumerate overpermissioned IAM roles; on Azure, use `az role assignment list --all` to identify accounts with Storage Blob Data Reader/Contributor on sensitive containers. Force password resets for all identified accounts via `Set-ADUser -ChangePasswordAtLogon $true`. Audit and revoke OAuth tokens and API keys for cloud services using your IdP's active token list — these persist independently of password resets and are a common persistence mechanism in data theft campaigns.

Evidence: Before rotating credentials, snapshot the current permission state of all cloud storage buckets and file shares (AWS S3 bucket policies, Azure RBAC assignments, SharePoint permission reports) to document the pre-eradication exposure surface — this establishes scope of potential data access for any required breach notification assessment. Capture a list of all OAuth tokens, API keys, and service account credentials currently active in your cloud

environment; in campaigns attributed to opportunistic groups like TheGentlemen and Nova, persistence via long-lived API tokens after initial credential compromise is a documented tactic. Preserve any cloud storage access logs showing specific files or directories accessed by compromised accounts — file paths and object names accessed during the breach window are essential for data impact scoping.

Step 4: Recovery — Verify MFA enforcement across all external-facing applications (CIS 6.3) and administrative accounts (CIS 6.5). Confirm audit logging is active and forwarding to a protected SIEM per NIST AU-9 (Protection of Audit Information) and CIS 8.2 (Collect Audit Logs). Monitor post-remediation for re-authentication attempts using previously valid credentials. Apply D3-CH (Credential Hardening) controls enterprise-wide.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection of Audit Information), NIST AU-12 (Audit Record Generation), NIST AC-7 (Unsuccessful Logon Attempts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 8.2 (Collect Audit Logs)

Compensating: Verify MFA coverage by querying your IdP for accounts lacking an enrolled MFA device: in Azure AD free tier, use `Get-MgUser -Filter 'accountEnabled eq true' | Get-MgUserAuthenticationMethod` to enumerate enrolled methods. For log integrity without a commercial SIEM, configure Windows Event Forwarding (WEF) to a dedicated hardened log collector and restrict write access to collector-only service accounts — this approximates AU-9 log protection at no cost. Set up osquery scheduled queries on critical endpoints to monitor for new local account creation (`SELECT * FROM users WHERE type='local'`) and new scheduled tasks, which would indicate re-compromise attempts. Configure alerting on Event ID 4771 (Kerberos pre-authentication failed) and 4776 (NTLM credential validation failed) to catch credential replay attempts using previously valid credentials rotated during eradication.

Evidence: During recovery validation, capture a baseline snapshot of all currently enrolled MFA devices per account from your IdP to confirm no attacker-enrolled authenticator apps or phone numbers persist — a technique used by threat actors to maintain authentication access after victim password resets. Preserve logs of all authentication events in the 72 hours post-credential-rotation, specifically looking for Event ID 4625 (Failed Logon) with sub-status 0xC000006A (wrong password) against recently rotated accounts, which would indicate an actor attempting replayed credentials. Document the restored permission state of cloud storage ACLs as a post-eradication baseline for future anomaly comparison.

Step 5: Post-Incident — Assess control gaps in phishing prevention (T1566 mitigation) and cloud data governance (T1530). If no data inventory exists, establish one per CIS 3.2 (Establish and Maintain a Data Inventory). Conduct a review of third-party and external system access policies per NIST AC-20 (Use of External Systems). Document findings and update incident playbooks to address opportunistic, multi-sector breach campaigns.

NIST Phase: Post Incident

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

Controls: NIST AC-20 (Use of External Systems), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 3.2 (Establish and Maintain a Data Inventory), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a T1566 control gap assessment using the free CISA Phishing Guidance checklist and verify DMARC, DKIM, and SPF DNS records for all owned domains using `dig TXT ` — misconfigured email authentication is a common enabler for phishing campaigns targeting non-technical sector organizations like those named in this advisory. For cloud data governance gap analysis without a CSPM, use the free tier of Prowler (open-source AWS/Azure/GCP security tool) to enumerate publicly accessible storage buckets and overpermissioned IAM roles: `prowler aws --compliance cis_level1_aws`. Document third-party vendor access (NIST AC-20) by auditing active site-to-site VPN tunnels and IdP federated trust relationships — investment holding companies and government food agencies commonly have broad third-party data sharing arrangements that expand the blast radius of credential-based breaches.

Evidence: For the lessons-learned record, compile the complete timeline of cloud storage access events attributed to compromised accounts, including exact object keys (file names) accessed — this drives the data impact scope determination required for breach notification under applicable regulations (India's DPDP Act for Anandji Haridas, Indonesia's PDP Law for Badan Pangan Nasional, and relevant GCC data protection frameworks for Arabian Procession Holding). Preserve the original phishing artifacts (email headers, attachment samples, URLs) if T1566 delivery was confirmed, and submit indicators to your national CERT (CERT-In for India, BSSN for Indonesia) per sector-specific reporting obligations. Document the pre-incident state of cloud ACLs, dormant account counts, and MFA coverage gaps as baseline metrics to measure remediation effectiveness and support playbook updates for future opportunistic multi-sector campaigns.

Detection Guidance

No confirmed IOCs are available for these incidents. Detection should focus on behavioral indicators consistent with the referenced MITRE techniques. For T1078 (Valid Accounts): query authentication logs for accounts logging in from new countries, new ASNs, or at atypical hours; flag accounts accessing more resources than their baseline. For T1566 (Phishing): review email gateway logs for messages with suspicious sender domains, lookalike display names, or links to credential-harvesting pages arriving near the claimed compromise window (late May to early June 2026). For T1530 (Data from Cloud Storage): alert on bulk download or export operations from cloud buckets or SharePoint/OneDrive by accounts not normally performing those actions. For T1119 (Automated Collection): look for scripted enumeration of file shares, databases, or directories, unusually high file-read counts from a single account in a short window. For T1041 (Exfiltration Over C2 Channel): monitor outbound traffic for large data transfers to uncommon external destinations, particularly to hosting providers or IP ranges not in your baseline. Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting). No verified IOC hashes, IPs, or domains are confirmed at time of writing; monitor threat intelligence feeds for TheGentlemen and Nova IOC publications.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`https://cybersecurityhunter.com/daily-cybersecurity-news-roundup-june-2-2026/`	T3 source reporting breach claims by TheGentlemen and Nova — not a malicious URL; secondary intelligence reference only	LOW
URL	`https://www.breachsense.com/breaches/page/2/`	T3 source aggregating recent breach claims including these incidents — not a malicious URL; secondary intelligence reference only	LOW

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1078** — Valid Accounts
- **T1530** — Data from Cloud Storage

- **T1119** — Automated Collection
- **T1566** — Phishing

NIST-800-53R5

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

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1530	Data from Cloud Storage	Collection
T1119	Automated Collection	Collection
T1566	Phishing	Initial-Access

Sources

Source	URL	Tier
Daily Cybersecurity News Roundup – June 2, 2026	https://cybersecurityhunter.com/daily-cybersecurity-news-roundup-ju...	T3
The Most Recent Data Breaches in 2026 - Breachsense	https://www.breachsense.com/breaches/page/2/	T3
[PDF] From Maps to Action - Global Alliance for Improved Nutrition	https://www.gainhealth.org/sites/default/files/publications/fsva-po...	T3
Indonesia Seeks Saudi Arabian Investment in Agricultural Projects	https://www.farmlandgrab.org/post/14096-indonesia-seeks-saudi-arabi...	T3
Food security challenges and opportunities in indonesia post COVID ...	https://pmc.ncbi.nlm.nih.gov/articles/PMC8459289/	T1

Generated 2026-06-04 06:48 UTC by TJS Security Command Center