INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-27 06:09 UTC

Bajaj Auto Hit by Ransomware Attack Impacting IT Operations

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0583
Type	Threat Campaign
Severity	HIGH
Affected Products	Bajaj Auto and Bajaj Auto Technology Limited, IT systems (specific systems not disclosed)
Published	2026-06-26
Discovery Source	Gemini

Executive Summary

Bajaj Auto and its subsidiary Bajaj Auto Technology Limited confirmed a ransomware attack discovered on the morning of June 24, 2026, affecting IT systems across both entities. The responsible threat group, ransom demand, and scope of any data exfiltration remain undisclosed as of initial reporting; operational impact is active (systems offline or services degraded) and scope under assessment by the vendor. Organizations with supply chain or partner dependencies on Bajaj Auto should treat this as an active third-party risk event until full scope is established.

Technical Analysis

Bajaj Auto and Bajaj Auto Technology Limited reported a ransomware incident affecting internal IT systems, discovered June 24, 2026. No CVE is associated; this is an operational ransomware deployment. Confirmed MITRE ATT&CK techniques map to: T1486 (Data Encrypted for Impact), T1489 (Service Stop), and T1490 (Inhibit System Recovery), the standard ransomware execution triad targeting backup infrastructure, recovery mechanisms, and service continuity. The initial access vector, ransomware family, and whether double-extortion (data exfiltration prior to encryption) occurred have not been publicly disclosed. Affected systems are described generically; no specific application, OS, or network segment has been named. Threat actor attribution is unknown. Patch status is not applicable, this is not a vulnerability-centric incident. No IOCs have been released by the company or third-party researchers as of initial reporting.

Action Checklist

1. Step 1: Containment, If your organization has active EDI, supplier portal, or data exchange connections with Bajaj Auto or Bajaj Auto Technology Limited, suspend or isolate those connections immediately pending confirmation of incident scope from the vendor. Segment any shared network zones per your network segmentation policy.
2. Step 2: Detection, Review endpoint detection and response (EDR) telemetry and SIEM logs for T1486 indicators (mass file rename events, Volume Shadow Copy deletion via vssadmin or wmic), T1489 indicators (unexpected service termination targeting backup agents or AV), and T1490 indicators (bcdedit or wbadmin command execution). Cross-reference against NIST AU-6 (Audit Record Review, Analysis, and Reporting) requirements for your own environment. CIS 8.2 requires audit logs to be collected across enterprise assets, confirm log ingestion is active for all critical systems.
3. Step 3: Eradication, No vendor-issued patch or configuration fix applies to this incident. For your own ransomware preparedness, confirm that backup systems are isolated from production networks per NIST CP-9 (System Backup) and that shadow copy and recovery mechanisms cannot be disabled by a standard user or compromised account. Enforce CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) to limit lateral movement potential.
4. Step 4: Recovery, If a partner-side compromise is confirmed to have propagated to your environment, initiate recovery from verified clean backups per NIST CP-10 (System Recovery and Reconstitution). Confirm backup integrity before restoration. Post-recovery, monitor for re-infection indicators and confirm that D3-CRO (Credential Rotation) has been applied to any accounts with access to shared systems or supplier integrations.
5. Step 5: Post-Incident, Conduct a third-party risk review for all manufacturing and automotive supply chain partners with IT system interdependencies. Map identified control gaps to NIST IR-4 (Incident Handling) to confirm your own preparation, detection, and containment procedures would catch a similar intrusion. Review whether your organization's ransomware playbook addresses supplier-originated propagation vectors.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to immediate priority and initiate full IR plan activation if any of the following are confirmed: encrypted files or ransom notes discovered on systems with EDI or supplier portal connectivity to Bajaj Auto, evidence of lateral movement from a supplier-connected network zone into production systems, or any account with access to shared Bajaj Auto integrations showing anomalous authentication events (Event ID 4624 Type 3 network logons, 4648 explicit credential use) after June 24, 2026; additionally, engage legal counsel and privacy officer if exfiltration of PII, PHI, or regulated data shared with Bajaj Auto is suspected, as breach notification obligations under applicable data protection regulations may be triggered.

Recovery Notes	Before restoring any system to production, validate backup integrity via hash comparison and scan restored images with YARA rules covering major ransomware families active in the automotive manufacturing sector; do not restore directly from a backup taken after June 24, 2026 without forensic verification that the backup itself was not captured during or after the compromise window. Post-restoration, maintain elevated monitoring for at least 30 days on all systems that had any network path to Bajaj Auto-connected zones, specifically watching for re-execution of `vssadmin delete shadows`, anomalous outbound connections to newly observed IPs, and service termination events targeting backup agents or AV processes. Confirm with Bajaj Auto's incident response team that they have achieved full eradication and that shared credentials or API keys used in supplier integrations have been rotated on their side before re-enabling any EDI or portal connections.
Forensic Artifacts	Windows Security Event Log entries (Event ID 4688 — Process Creation) for `vssadmin.exe delete shadows`, `wbadmin delete catalog`, `bcdedit /set recoveryenabled no`, and `wmic shadowcopy delete` commands executed in the window surrounding June 24, 2026 on any host with supplier portal or EDI network access — these are the canonical ransomware pre-encryption preparation commands and their presence confirms active or imminent encryption activity. | Sysmon Event ID 11 (FileCreate) logs showing mass file rename or creation events with ransom-associated extensions (e.g., `.locked`, `.encrypted`, `.ransom`, or a campaign-specific extension not yet disclosed) or ransom note filenames (e.g., `README.txt`, `DECRYPT_FILES.html`, `HOW_TO_RECOVER.txt`) across user-writable network shares and local drives, which identifies the encryption blast radius. | EDI gateway and supplier portal access logs (application-layer logs from your B2B integration platform, AS2 gateway, or API management layer) covering the 14 days prior to June 24, 2026, reviewed for anomalous file transfer volumes, unexpected data types, or connections originating from Bajaj Auto infrastructure outside normal business hours — these may reveal the initial vector if compromise propagated inbound through the integration channel. | Windows VSS and backup service event logs (Application Event Log, VSS provider Event IDs 8193 and 8194; Backup Operators group audit events; any backup agent service crash or unexpected stop events) to determine whether shadow copies and recovery mechanisms were destroyed before or after encryption began, establishing attacker dwell time and sequencing. | Network perimeter firewall and proxy logs for all outbound connections from supplier-connected network zones to external IPs in the 72 hours surrounding June 24, 2026, filtered for large-volume data transfers or beaconing patterns to uncommon destinations — relevant to assessing whether data exfiltration accompanied the ransomware deployment, consistent with double-extortion tactics common in 2025–2026 ransomware campaigns targeting manufacturing sector organizations.

Per-Action IR Details

Step 1: Containment — If your organization has active EDI, supplier portal, or data exchange connections with Bajaj Auto or Bajaj Auto Technology Limited, suspend or isolate those connections immediately pending confirmation of incident scope from the vendor. Segment any shared network zones per your network segmentation policy.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use Windows Firewall with Advanced Security (wf.msc) or iptables to block all inbound/outbound traffic to Bajaj Auto IP ranges and EDI gateway endpoints immediately. Run `netstat -ano | findstr ESTABLISHED` (Windows) or `ss -tunap` (Linux) to enumerate active sessions to supplier endpoints before cutting the connection, and

document all established sessions for forensic record.

Evidence: Before suspending connections, capture full network state: run `Get-NetTCPConnection | Where-Object State -eq 'Established' | Export-Csv -Path C:\IR\net_connections_$(Get-Date -Format yyyyMMddHHmm).csv` to record all active sessions to Bajaj Auto-affiliated IP ranges. Capture firewall logs (Windows Event IDs 5156/5157 for allowed/blocked connections, or perimeter firewall syslog) showing historical EDI/supplier portal traffic patterns for the 30 days prior to June 24, 2026. Preserve any EDI transaction logs or supplier portal session tokens before isolation, as these may reveal whether a lateral pivot originated from the Bajaj Auto side.

Step 2: Detection — Review endpoint detection and response (EDR) telemetry and SIEM logs for T1486 indicators (mass file rename events, Volume Shadow Copy deletion via vssadmin or wmic), T1489 indicators (unexpected service termination targeting backup agents or AV), and T1490 indicators (bcdedit or wbadmin command execution). Cross-reference against NIST AU-6 (Audit Record Review, Analysis, and Reporting) requirements for your own environment. CIS 8.2 requires audit logs to be collected across enterprise assets — confirm log ingestion is active for all critical systems.

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), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity's configuration to capture Event ID 1 (Process Create) for `vssadmin.exe delete shadows`, `wmic shadowcopy delete`, `bcdedit /set recoveryenabled no`, and `wbadmin delete catalog`. Use the following PowerShell query against the Windows Security Event Log: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'vssadmin|wmic|bcdedit|wbadmin'}`. For Linux hosts, grep `/var/log/auth.log` and `/var/log/syslog` for shadow deletion equivalents. Apply the public Sigma rule `ransomware_delete_volume_shadow_copies.yml` if using a log aggregator such as Graylog or Elastic.

Evidence: This is a detection/analysis step that does not alter live state, but if an active infection is suspected on any host during this review, capture volatile memory (using WinPmem or Magnet RAM Capture) and running process list (`Get-Process | Export-Csv`) before any remediation action. Key artifacts to query: Windows Security Event Log Event ID 4688 (process creation) for `vssadmin.exe`, `wmic.exe`, `bcdedit.exe`, `wbadmin.exe`; Sysmon Event ID 11 (FileCreate) for mass `.encrypted`, `.locked`, or ransom-note filename patterns in user-writable shares; Windows Application Event Log for VSS provider errors (Event ID 8193, 8194); and any EDR telemetry showing backup agent service termination events correlated with the June 24, 2026 discovery window.

Step 3: Eradication — No vendor-issued patch or configuration fix applies to this incident. For your own ransomware preparedness, validate that backup systems are isolated from production networks per NIST CP-9 (System Backup) and that shadow copy and recovery mechanisms cannot be disabled by a standard user or compromised account. Enforce CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts) to limit lateral movement potential.

NIST Phase: Eradication

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

Controls: NIST CP-9 (System Backup), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process)

Compensating: Run `Get-LocalGroupMember -Group Administrators` on all Windows endpoints to audit local admin membership and remove non-dedicated accounts. Use `vssadmin list shadows` to verify that shadow copies still exist and have not been deleted. For backup isolation verification, confirm backup server network interfaces are on a dedicated VLAN with no route from production; use `route print` or `ip route show` to validate on backup hosts. Set a Group Policy Object (GPO) to restrict `vssadmin` and `wbadmin` execution to SYSTEM and dedicated backup service accounts only via Software Restriction Policy or AppLocker.

Evidence: Before making any privilege changes or GPO modifications that alter system state, capture: current local administrator group membership (`Get-LocalGroupMember -Group Administrators | Export-Csv`), list of currently active privileged sessions (`qwinsta` and `Get-PSSession`), and a full export of existing VSS shadow copies (`vssadmin list

shadows > C:\IR\vss_snapshot_$(Get-Date -Format yyyyMMddHHmm).txt`). If any host is suspected of active compromise during this eradication validation, acquire RAM with WinPmem before any account or privilege changes, as ransomware operators frequently maintain persistence via injected threads in LSASS or legitimate system processes that will be lost on reboot or session termination.

Step 4: Recovery — If a partner-side compromise is confirmed to have propagated to your environment, initiate recovery from verified clean backups per NIST CP-10 (System Recovery and Reconstitution). Validate backup integrity before restoration. Post-recovery, monitor for re-infection indicators and confirm that D3-CRO (Credential Rotation) has been applied to any accounts with access to shared systems or supplier integrations.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST CP-10 (System Recovery And Reconstitution), NIST CP-9 (System Backup), CIS 5.2 (Use Unique Passwords)

Compensating: Before restoring from backup, validate backup integrity by computing SHA-256 hashes of backup archives and comparing against stored manifests: `Get-FileHash -Algorithm SHA256 -Path `. Restore to an isolated staging environment first and run a YARA scan against restored files using public ransomware family YARA rules (e.g., from the Malpedia YARA repository) to confirm the backup is clean before promoting to production. Rotate all credentials for accounts that had access to Bajaj Auto supplier portals, EDI gateways, or shared integration systems using `net user /domain` or the IdP admin console, and invalidate all active sessions via Azure AD `Revoke-AzureADUserAllRefreshToken` or equivalent.

Evidence: Before initiating any restore operation or credential rotation that alters live state, capture: full memory image of any affected host (WinPmem), active network connections (`Get-NetTCPConnection | Export-Csv`), list of encrypted files and ransom note locations (`Get-ChildItem -Recurse | Where-Object {$_.Name -match 'README|DECRYPT|\.locked|\.encrypted'} | Export-Csv`), and all Windows Security Event Log entries for the compromise window (Event ID 4624/4625 logon events, 4648 explicit credential use, 4776 NTLM authentication) covering the period from June 24, 2026 onward. These artifacts establish the blast radius and credential exposure scope required before D3-CRO credential rotation is applied.

Step 5: Post-Incident — Conduct a third-party risk review for all manufacturing and automotive supply chain partners with IT system interdependencies. Map identified control gaps to NIST IR-4 (Incident Handling) to confirm your own preparation, detection, and containment procedures would catch a similar intrusion. Review whether your organization's ransomware playbook addresses supplier-originated propagation vectors.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Produce a tabletop exercise scenario modeled on the Bajaj Auto incident — ransomware propagating inbound from a supplier EDI connection — and walk the IR team through detection, containment, and escalation decision points using only free tooling (Sysmon, osquery, Wireshark). Use osquery's `process_open_sockets` and `listening_ports` tables to baseline all supplier integration endpoints and export results for a before/after comparison in future incidents. Document all third-party IT dependencies in a simple spreadsheet (partner name, connection type, network zone, data exchanged, last security review date) as a minimum viable third-party risk inventory.

Evidence: This post-incident phase does not involve live system changes requiring volatile capture; however, retain and archive all forensic artifacts collected during Steps 1–4 per your evidence retention policy, including: network flow logs covering the June 24, 2026 discovery date, all EDR telemetry exports, credential access logs for shared supplier accounts, and any ransom note or encrypted file samples if propagation reached your environment. These artifacts are required to complete the lessons-learned report, support any regulatory breach notification assessment, and enable threat intelligence sharing with ISACs relevant to the automotive manufacturing sector (e.g., Auto-ISAC).

Detection Guidance

In your own environment, hunt for the T1486/T1489/T1490 execution triad: (1) Volume Shadow Copy deletion, query for vssadmin.exe delete shadows, wmic.exe shadowcopy delete, or bcdedit.exe /set {default} recoveryenabled No in process creation logs (Windows Event ID 4688 or Sysmon Event ID 1); (2) Mass file rename or extension change events, file system auditing showing high-volume rename activity within short time windows, particularly targeting document, database, and backup directories; (3) Backup agent service termination, monitor for unexpected stops of services associated with your backup solution (Windows Event ID 7036, service name changes). For third-party exposure monitoring, obtain Bajaj Auto's published IP ranges (via WHOIS or ASN lookup) and watch for anomalous outbound connections to those ranges or supplier portal endpoints. No public IOCs (hashes, IPs, domains, ransom note filenames) have been released for this incident. Per NIST AU-6, review audit records at defined frequency for these behavioral patterns. D3-SFA (System File Analysis) and D3-LAM (Local Account Monitoring) are applicable countermeasures for early detection.

Framework Mappings

MITRE-ATTACK

- **T1489** — Service Stop
- **T1490** — Inhibit System Recovery
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling
- **AT-2** — Literacy Training and Awareness

NIST-CSF-2

- **RS.MI-01** — Incidents are contained

HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1489	Service Stop	Impact
T1490	Inhibit System Recovery	Impact
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Bajaj Auto security incident: ransomware attack impacts IT systems	https://www.upguard.com/news/bajaj-auto-data-breach-2026-06-24	T3
Bajaj Auto Confirms Systems Affected by Ransomware Attack ...	https://x.com/The_Cyber_News/status/2069468436254867673	T3
Indian auto giant Bajaj Auto hit by ransomware incident	https://therecord.media/indian-auto-giant-bajaj-auto-hit-by-ransomware	T3
Bajaj Auto Hit By Ransomware Attack; Impact On Operations Under ...	https://www.youtube.com/watch?v=JlskSdf-aUI	T3
Bajaj Auto Confirms Systems Affected by Ransomware Attack	https://securityboulevard.com/2026/06/bajaj-auto-confirms-systems-a...	T3

Generated 2026-06-27 06:09 UTC by TJS Security Command Center