INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-16 19:20 UTC

# Ransomware Attack Disrupts Operations at Australian Sugar Producer Mackay Sugar

THREAT CAMPAIGN | HIGH

| | |
|---|---|
| SCC Item ID | SCC-CAM-2026-0489 |
| Type | Threat Campaign |
| Severity | HIGH |
| Affected Products | Mackay Sugar (Australian sugar producer, second-largest in Australia), operational technology and business systems |
| Published | 2026-06-15 |
| Discovery Source | Gemini |

## Executive Summary

Mackay Sugar, Australia's second-largest sugar producer, suffered a ransomware attack that forced shutdowns at multiple North Queensland sugar mills, disrupting both IT and operational technology environments. The attack demonstrates continued threat actor targeting of food and agriculture critical infrastructure, where OT disruptions translate directly to production losses and supply chain impact. Attribution and initial access vector remain unconfirmed; the incident is covered by secondary sources with medium confidence in ransomware classification.

## Technical Analysis

A ransomware attack impacted Mackay Sugar's IT and operational technology (OT) environments, resulting in mill shutdowns across multiple North Queensland facilities. MITRE ATT&CK techniques observed or associated with this incident class include T1486 (Data Encrypted for Impact), T1490 (Inhibit System Recovery), and T1657 (Financial Theft). No CVE identifier is associated with this campaign. Initial access vector, ransomware family, and any data exfiltration scope have not been publicly confirmed. No authoritative advisory from ACSC, CISA, or equivalent government body has been matched to this event. Source coverage is T3 (ABC News, LinkedIn, Reddit, Instagram); no primary government or vendor advisory is available. Confidence in ransomware classification: medium. OT environment impact suggests the ransomware propagated beyond standard IT network boundaries, consistent with IT/OT convergence risk patterns, though the lateral movement path has not been disclosed.

## Action Checklist

1. Step 1: Containment. Conduct an immediate audit of IT/OT network segmentation to confirm that industrial control systems and mill operations networks are not reachable from corporate IT segments. Isolate any systems showing anomalous encryption activity or backup deletion (T1490, T1486). Apply CIS 4.4 and CIS 4.5 firewall controls to enforce default-deny between IT and OT zones.
2. Step 2: Detection. Query endpoint and SIEM logs for mass file rename events, Volume Shadow Copy deletion commands (vssadmin delete shadows, wmic shadowcopy delete), and disabling of backup agents. Monitor for unusual process execution on OT historian or HMI hosts. Reference NIST AU-6 (Audit Record Review) and AU-2 (Event Logging) to ensure OT-side logging is active and forwarded to your central log platform. Apply system file analysis to detect modification of system executables or configuration files on OT assets.
3. Step 3: Eradication. No specific patch or vendor advisory is available for this campaign. Eradication steps follow standard ransomware response: identify and isolate affected hosts, terminate malicious processes, remove persistence mechanisms (check scheduled tasks, startup entries per NIST controls), and rotate all credentials that may have been exposed. Rebuild affected systems from known-good images rather than attempting in-place recovery.
4. Step 4: Recovery. Restore operations from verified, offline backups consistent with NIST CP-9 (System Backup) and CP-10 (System Recovery and Reconstitution). Before reconnecting OT systems, validate integrity of ICS/SCADA configurations. Monitor restored systems for re-infection indicators for a minimum of 30 days post-recovery. Ensure audit logging (NIST AU-12, CIS 8.2) is confirmed active across all restored assets before returning to production.
5. Step 5: Post-Incident. Conduct a formal lessons-learned review under NIST IR-4 (Incident Handling) and IR-8 (Incident Response Plan). Assess IT/OT segmentation gaps, backup coverage for OT environments, and detection coverage on non-standard OT endpoints. Validate MFA is enforced on all remote access paths per CIS 6.4 and CIS 6.5. Review whether dormant or default accounts in OT environments were exploited per CIS 5.3 and CIS 4.7.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate immediately if OT network isolation cannot be confirmed within 2 hours, if ransomware encryption is detected on ICS historian or HMI hosts controlling active mill crushing or processing operations, or if the incident triggers mandatory reporting obligations under Australia's Security of Critical Infrastructure Act 2018 — food and agriculture operators above the relevant threshold must notify the Australian Cyber Security Centre (ACSC). |
| **Recovery Notes** | Prioritize restoration of OT historian and SCADA systems over corporate IT, as continued mill downtime during Queensland sugar crushing season translates directly to perishable cane losses and contract penalties. Before returning any OT system to production, independently verify PLC program integrity against vendor-provided checksums or pre-incident offline copies — ransomware actors targeting industrial environments have been observed modifying ICS configurations as a secondary impact. Maintain elevated monitoring (osquery scheduled queries, Sysmon Event ID 1 and 11 alerting) on all restored OT hosts for a minimum of 30 days, as ransomware affiliates targeting food and agriculture critical infrastructure have demonstrated re-entry through unpatched remote access paths left open after initial recovery. |

| | |
|---|---|
| **Forensic Artifacts** | Windows Security Event Log (Event ID 4688 — Process Creation) on OT historian and HMI hosts showing execution of vssadmin.exe, wmic.exe, bcdedit.exe, or net.exe — these are the primary indicators of ransomware pre-encryption activity in Windows-based ICS environments such as those used at Mackay Sugar mills \| Master File Table ($MFT) and $UsnJrnl ($J) from affected Windows hosts, captured via KAPE or Velociraptor, to reconstruct the ransomware file encryption timeline across OT project directories (PLC backup folders, SCADA historian data paths, HMI project files) \| OSIsoft PI Server or equivalent OT historian audit logs showing unexpected data archive access, historian service restarts, or bulk tag deletion events coinciding with the ransomware deployment window \| Network flow logs or firewall logs (pfSense, Windows Firewall) from the IT/OT boundary showing lateral movement from corporate IP ranges into mill operations VLAN subnets — critical for establishing how ransomware traversed from business systems into the Mackay Sugar OT environment \| Volatile memory images (WinPMEM/DumpIt) from any host where ransomware processes were observed running, preserving in-memory ransomware binary artifacts, encryption key material, and C2 connection state that are unrecoverable after process termination or system reboot |

### Per-Action IR Details

**Step 1: Containment — Immediately audit IT/OT network segmentation to confirm that industrial control systems and mill operations networks are not reachable from corporate IT segments. Isolate any systems showing anomalous encryption activity or backup deletion (T1490, T1486). Apply CIS 4.4 and CIS 4.5 firewall controls to enforce default-deny between IT and OT zones.**

**NIST Phase:** Containment

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

**Controls:** CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

**Compensating:** On Windows OT jump hosts and historian servers, run `netstat -ano` and `Get-NetTCPConnection` to enumerate active connections from corporate subnets to OT VLAN ranges. Use pfSense or Windows Firewall with Advanced Security (netsh advfirewall) to enforce deny-all inbound from IT segments to OT VLAN — document every rule change with a timestamp. On Linux-based HMI or historian hosts, run `ss -tulnp` and apply iptables DROP rules for corporate IP ranges.

**Evidence:** BEFORE isolating any host, capture full RAM image using WinPMEM or DumpIt from potentially compromised IT-side pivot hosts, and capture `Get-NetTCPConnection | Where-Object {$_.State -eq 'Established'}` output showing live sessions into the OT network. Record arp cache (`arp -a`) and routing tables (`route print`) to map lateral movement paths from IT to OT. Ransomware targeting OT environments frequently stages on IT-side hosts before pivoting — live connection state between corporate and mill operations networks is destroyed the moment you apply firewall rules or isolate hosts.

**Step 2: Detection — Query endpoint and SIEM logs for mass file rename events, Volume Shadow Copy deletion commands (vssadmin delete shadows, wmic shadowcopy delete), and disabling of backup agents. Monitor for unusual process execution on OT historian or HMI hosts. Reference NIST AU-6 (Audit Record Review) and AU-2 (Event Logging) to ensure OT-side logging is active and forwarded to your central log platform. Apply D3-SFA (System File Analysis) to detect modification of system executables or configuration files on OT assets.**

**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), CIS 8.2 (Collect Audit Logs)

**Compensating:** Deploy Sysmon with SwiftOnSecurity config on all Windows-based OT historian and HMI hosts; specifically, enable Event ID 1 (Process Create) to catch `vssadmin.exe` and `wmic.exe` invocations, and Event ID 11 (FileCreate) to detect mass `.encrypted` or ransom-note file writes in OT project directories (e.g., `C:\Program Files\Wonderware`, `C:\PLC Backups`). Run this PowerShell query against Windows Event Logs on OT hosts: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4688 -and $_.Message -match 'vssadmin|wmic|bcdedit'}`. For Linux historians, use `auditd` with a rule watching `/var/log/` and ICS configuration paths for bulk modification: `auditctl -w /opt/ignition -p wa -k ot_tampering`.

**Evidence:** BEFORE any remediation action, preserve Windows Security Event Log (Event ID 4688 — Process Creation, Event ID 4663 — Object Access) and Sysmon logs from OT historian and HMI hosts showing `vssadmin delete shadows` or `wmic shadowcopy delete` execution. Capture the contents of `C:\Windows\System32\Tasks` and `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Schedule\TaskCache` to document persistence mechanisms. Collect OT-specific logs: OSIsoft PI Server audit logs (if deployed as historian), Wonderware InTouch application logs, and GE iFIX event logs showing unexpected shutdowns or configuration changes. These volatile process execution records are overwritten as Windows recycles the event log buffer.

**Step 3: Eradication — No specific patch or vendor advisory is available for this campaign. Eradication steps follow standard ransomware response: identify and isolate affected hosts, terminate malicious processes, remove persistence mechanisms (check scheduled tasks, startup entries per D3-SICA), and rotate all credentials that may have been exposed (D3-CRO). Rebuild affected systems from known-good images rather than attempting in-place recovery.**

**NIST Phase:** Eradication

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

**Controls:** NIST IR-4 (Incident Handling), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

**Compensating:** Use Autoruns (Sysinternals) on any OT Windows host prior to reimaging to document all persistence points — pay particular attention to `HKLM\SYSTEM\CurrentControlSet\Services` for ransomware-installed services and `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run` for startup entries. Export the full Autoruns log to a forensic share before wiping. For credential rotation in OT environments without AD, enumerate local accounts on each HMI and historian using `net user` and `Get-LocalUser`, then reset all passwords; for OT service accounts, update credentials in the OT vendor's configuration manager (e.g., Ignition Gateway, PI AF) before reconnecting to the network.

**Evidence:** BEFORE terminating processes or reimaging: acquire a full RAM image (WinPMEM/DumpIt) from each affected host to preserve in-memory ransomware binary and decryption key material — this is the only opportunity to recover encryption keys if a decryptor is later developed for this campaign. Capture a prefetch snapshot (`C:\Windows\Prefetch\`) and `$MFT` (Master File Table) via a forensic tool such as Velociraptor or KAPE to establish a ransomware execution timeline specific to the Mackay Sugar mill environment. Document all encrypted OT project files and their paths (e.g., PLC ladder logic backups, SCADA screen definitions) to assess OT configuration data loss scope before wiping.

**Step 4: Recovery — Restore operations from verified, offline backups consistent with NIST CP-9 (System Backup) and CP-10 (System Recovery and Reconstitution). Before reconnecting OT systems, validate integrity of ICS/SCADA configurations. Monitor restored systems for re-infection indicators for a minimum of 30 days post-recovery. Ensure audit logging (NIST AU-12, CIS 8.2) is confirmed active across all restored assets before returning to production.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST CP-9 (System Backup), NIST CP-10 (System Recovery And Reconstitution), CIS 8.2 (Collect Audit Logs)

**Compensating:** Before reconnecting any restored OT host, run a YARA scan using a community ransomware rule set (e.g., Arkbird or Malpedia YARA rules) against restored disk images to confirm no dormant ransomware binary survived in OT software directories. Validate ICS/SCADA configuration integrity by comparing SHA-256 hashes of restored PLC program files and HMI project files against pre-incident hashes stored offline — use `certutil -hashfile

SHA256` on Windows or `sha256sum` on Linux. Deploy osquery on restored OT hosts with a query scheduled every 15 minutes to watch for new scheduled tasks, service installs, and VSS deletion attempts during the 30-day monitoring window.

**Evidence:** BEFORE reconnecting restored systems to the OT network, verify that offline backup media has not been encrypted by confirming backup file headers match vendor-expected formats (e.g., OSIsoft PI backup `.bak` headers, Ignition Gateway `.gwbk` ZIP structure). Ransomware targeting food and agriculture OT environments has been observed pre-staging on backup infrastructure — validate backup server integrity independently before trusting restore sources. Document the hash and timestamp of each restored OT configuration file as a forensic baseline for the 30-day monitoring period.

**Step 5: Post-Incident — Conduct a formal lessons-learned review under NIST IR-4 (Incident Handling) and IR-8 (Incident Response Plan). Assess IT/OT segmentation gaps, backup coverage for OT environments, and detection coverage on non-standard OT endpoints. Validate MFA is enforced on all remote access paths per CIS 6.4 and CIS 6.5. Review whether dormant or default accounts in OT environments were exploited per CIS 5.3 and CIS 4.7.**

**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 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.3 (Disable Dormant Accounts), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

**Compensating:** Run `net user /domain` and `Get-ADUser -Filter {Enabled -eq $true -and LastLogonDate -lt (Get-Date).AddDays(-45)}` to identify dormant accounts that may have been used for initial access or lateral movement into the Mackay Sugar OT environment. For OT-specific default accounts (Wonderware, Ignition, OSIsoft PI), consult each vendor's hardening guide and audit local account lists on every historian and HMI using `Get-LocalUser`. Document the IT/OT segmentation state as-found (firewall rules, VLAN assignments, unmanaged switches in mill floor networks) as the primary artifact for the lessons-learned report — sugar mill OT environments frequently have legacy flat networking inherited from pre-IT/OT convergence deployments.

**Evidence:** Preserve the complete incident timeline documentation including: all firewall and switch logs showing IT-to-OT traffic paths used during the attack, AD authentication logs (Event ID 4624, 4625, 4648) covering the 30 days prior to detection to identify the initial access account, and any VPN or remote access gateway logs that may reveal the attacker's entry point into Mackay Sugar's corporate network. These records support both the internal lessons-learned process and any mandatory reporting obligations to the Australian Cyber Security Centre (ACSC) under Australia's Security of Critical Infrastructure Act 2018, which covers food and agriculture as a designated critical infrastructure sector.

## Detection Guidance

Detection for this campaign class should focus on ransomware behavioral indicators, particularly in environments with IT/OT convergence. Key signals to hunt: (1) Volume Shadow Copy deletion via vssadmin.exe or wmic.exe with shadowcopy delete arguments; (2) mass file extension changes or rapid file modification events across shared drives and OT data historians; (3) backup agent service termination or disabling of Windows Backup and restore processes; (4) anomalous lateral movement from IT subnets toward OT VLAN segments, particularly toward historian servers, HMIs, or engineering workstations; (5) T1490 indicators, disabling of recovery mode, bcdedit /set {default} recoveryenabled No. NIST AU-6 and AU-2 require these event types to be logged and reviewed at defined frequencies. CIS 8.2 requires audit log collection to be enabled across all enterprise assets, including OT-adjacent systems. No confirmed IOCs (IPs, domains, hashes) have been publicly released for this incident. Apply local account monitoring to detect privilege escalation or unauthorized local account activity on OT hosts. No authoritative ACSC or CISA advisory has been matched to this event; monitor ACSC advisories at cyber.gov.au for any formal notification.

## Framework Mappings

### MITRE-ATTACK

- **T1490** — Inhibit System Recovery
- **T1486** — Data Encrypted for Impact
- **T1657** — Financial Theft

### NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling

### NIST-CSF-2

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

### HIPAA-SECURITY

- **164.308(a)(7)(ii)(A)** — Data Backup Plan

### ISO-27001-2022

- **A.5.29** — Information security during disruption

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1490 | Inhibit System Recovery | Impact |
| T1486 | Data Encrypted for Impact | Impact |
| T1657 | Financial Theft | Impact |

## Sources

| Source | URL | Tier |
|---|---|---|
| **gemini** | https://securityaffairs.com/174987/security/cve-2026-20262-cisco-ca... | T3 |
| **Cyber attack shuts down two Mackay Sugar mills - ABC News** | https://www.abc.net.au/news/2026-06-10/cyber-attack-shuts-down-nort... | T3 |
| **Cyberattack disrupts Mackay Sugar operations, exposing growing ...** | https://www.linkedin.com/pulse/cyberattack-disrupts-mackay-sugar-op... | T3 |

| Source | URL | Tier |
|---|---|---|
| **Ransomware Attack Shuts Down Mills of Australia's Second-Largest ...** | https://www.reddit.com/r/cybersecurity/comments/1u6ka5m/ransomware_... | T3 |
| **Mackay sugar cyberattack disrupts operations, halts ... - Instagram** | https://www.instagram.com/p/DZcrR3MgdmU/ | T3 |