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

Global Ransomware Campaign Targets Government, Education, and Private Sector Organizations

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0488
Type	Threat Campaign
Severity	HIGH
Affected Products	Röben Tonbaustoffe GmbH (Germany), Kedah State Government (Malaysia), Illinois Central College (US), Moody Bible Institute (US), Glendale Community College (US), TheCreditPros (US), SPORTON International Inc. (Taiwan)
Published	2026-06-16
Discovery Source	Gemini

Executive Summary

A wave of ransomware incidents has struck seven organizations across Germany, Malaysia, the United States, and Taiwan, spanning government, education, manufacturing, financial services, and testing and certification sectors. Attackers appear to have used double-extortion tradecraft, exfiltrating data before encrypting systems and threatening public release to pressure victims into paying. Any organization in these sectors should treat this as an active threat signal, particularly those with internet-facing infrastructure or limited endpoint detection capabilities.

Technical Analysis

This campaign represents a geographically distributed ransomware operation affecting Röben Tonbaustoffe GmbH (Germany), Kedah State Government (Malaysia), Illinois Central College, Moody Bible Institute, Glendale Community College, TheCreditPros (US), and SPORTON International Inc. (Taiwan). Reported tradecraft is consistent with double-extortion ransomware: initial access via phishing (T1566) or valid account abuse (T1078), followed by data exfiltration over C2 channels (T1041), data encryption for impact (T1486), and financial extortion (T1657). No specific ransomware group has been attributed, no technical IOCs have been confirmed, and no CVE or CWE identifiers are associated with this campaign at this time. Source data originates from Ransomware.live (T3 aggregator) with Gemini as a secondary discovery source. Technical intrusion vectors, ransomware families, ransom amounts, and confirmed exfiltration volumes remain unverified in available source material.

Action Checklist

1. Containment: Audit and restrict internet-facing RDP, VPN endpoints, and remote access services immediately. Enforce network segmentation to limit lateral movement potential from any compromised endpoint. Apply CIS 4.4 and CIS 4.5 to verify host-based firewall configurations on servers and end-user devices are enforcing default-deny rules.
2. Detection: Hunt for anomalous authentication events using NIST AU-2 event logging baselines: look for off-hours logons, logons from unexpected geographies, and privilege escalation from standard user accounts. Query endpoint and SIEM logs for large outbound data transfers consistent with T1041 exfiltration patterns. Apply D3-LAM (Local Account Monitoring) to flag unusual local account activity and new account creation.
3. Eradication: Rotate credentials on any accounts showing anomalous access per D3-CRO (Credential Rotation). Disable or remove unneeded accounts per CIS 5.3 (Disable Dormant Accounts). Enforce MFA on all remote access per CIS 6.4 and on all administrative accounts per CIS 6.5 to close the T1078 valid accounts vector.
4. Recovery: Validate backup integrity and test restoration procedures before returning affected systems to production. Monitor restored systems with enhanced logging per NIST AU-6 (Audit Record Review, Analysis, and Reporting). Confirm audit log storage capacity is sufficient for extended retention under NIST AU-4 and AU-11.
5. Post-Incident: Conduct a gap assessment against CIS 7.1 (Vulnerability Management Process) and CIS 7.2 (Remediation Process) to identify unpatched systems that may have served as initial access points. Review phishing resilience controls mapped to T1566 and document lessons learned for playbook updates, particularly for sectors matching those targeted in this campaign.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal counsel if any confirmed exfiltration of PII, student records (FERPA), or financial data is identified, as breach notification obligations apply across multiple jurisdictions represented by the affected organizations (Germany GDPR, US state breach laws, Malaysia PDPA), or if ransomware detonation is confirmed on any host — active encryption constitutes a declared incident under NIST 800-61r3 §3.2 incident criteria.
Recovery Notes	Before returning any system to production, confirm that the backup set used for restoration predates the earliest confirmed attacker access timestamp, and that no ransomware persistence mechanisms (scheduled tasks, autorun registry keys, or implanted web shells on internet-facing services) survive on restored hosts. Given the double-extortion tradecraft observed in this campaign, elevated monitoring of outbound data transfers and authentication events must remain in place for a minimum of 30 days post-restoration, as operators may retain access through secondary backdoors planted during the exfiltration phase. Organizations in government, education, and financial services matching the victim profile should coordinate with their sector ISAC to determine whether shared IOCs from confirmed victims can accelerate detection of residual attacker infrastructure.

Forensic Artifacts	Windows Security Event Log — Event IDs 4624 (Logon Type 10: RemoteInteractive), 4625, 4648, 4720, and 4732 from all internet-facing and domain controller hosts, covering 90 days pre-incident to reconstruct the double-extortion dwell period and initial access vector (RDP/VPN credential abuse). | Ransomware binary and ransom note artifacts — file system forensics targeting %TEMP%, %APPDATA%, C:\ProgramData, and web server root directories for dropper executables, ransom note text files (commonly named README.txt, DECRYPT_FILES.html, or variant-specific names), and encrypted file extension patterns left by the specific ransomware family deployed in this campaign. | VSS (Volume Shadow Copy) deletion events — Windows System Event Log Event ID 7036 and Security Event ID 4688 filtering on vssadmin.exe, wmic.exe, and powershell.exe with arguments containing 'delete shadows', 'resize shadowstorage', or 'Win32_ShadowCopy' — deletion of shadow copies is a near-universal precursor to encryption in the ransomware families targeting government and education sectors. | Network flow and proxy logs — firewall and proxy logs for large-volume outbound transfers (>1 GB) to non-business IPs in the 30 days preceding encryption, DNS query logs for DGA-like domains or known ransomware C2 infrastructure, and any SFTP, FTP, rclone, or MEGAcmd process network connections consistent with double-extortion exfiltration tooling. | Active Directory replication and privileged account audit logs — Event IDs 4769 (Kerberos service ticket), 4776 (NTLM credential validation), and 4728/4732 (group membership changes) on domain controllers, to identify whether the ransomware operator achieved domain-level privilege escalation across the targeted organization's environment prior to deploying encryption payloads.

Per-Action IR Details

Containment — Audit and restrict internet-facing RDP, VPN endpoints, and remote access services immediately. Enforce network segmentation to limit lateral movement potential from any compromised endpoint. Apply CIS 4.4 and CIS 4.5 to verify host-based firewall configurations on servers and end-user devices are enforcing default-deny rules.

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), NIST AC-17 (Remote Access), NIST AC-4 (Information Flow Enforcement)

Compensating: Run `netstat -ano | findstr :3389` and `netstat -ano | findstr LISTEN` on all Windows hosts to enumerate exposed RDP listeners; pipe output to a file for comparison. Use Windows Firewall (`netsh advfirewall firewall`) to block inbound TCP 3389 and common VPN ports (UDP 500, 4500, TCP 1194, 443 for SSL-VPN) on endpoints lacking EDR. Deploy Sysmon with SwiftOnSecurity ruleset to capture network connection events (Event ID 3) for ongoing lateral movement detection.

Evidence: Before restricting or reconfiguring any remote access service, capture: (1) full `netstat -ano` output and active RDP session list (`query session /server:`) to record all live connections and session owners; (2) Windows Security Event Log entries — Event ID 4624 (successful logon, Logon Type 10 = RemoteInteractive), 4625 (failed logon), and 4778/4779 (RDP session reconnect/disconnect) from all internet-facing hosts; (3) VPN gateway authentication logs showing source IPs, usernames, and session timestamps; (4) firewall flow logs for inbound TCP 3389 and VPN ports over the prior 30 days to establish the initial access timeline for this campaign's double-extortion tradecraft.

Detection — Hunt for anomalous authentication events using NIST AU-2 event logging baselines: look for off-hours logons, logons from unexpected geographies, and privilege escalation from standard user accounts. Query endpoint and SIEM logs for large outbound data transfers consistent with T1041 exfiltration patterns. Apply D3-LAM (Local Account Monitoring) to flag unusual local account activity and new account creation.

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-3 (Content Of Audit Records)

Compensating: Without a SIEM, use PowerShell to query the Security event log directly: `Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4625,4720,4732,4728)} | Select-Object TimeCreated,Message | Export-Csv auth_hunt.csv`. For exfiltration detection, run Wireshark or `netstat -b 5` to identify processes sustaining large outbound connections, and check Windows Security Event ID 5156 (Windows Filtering Platform connection allowed) for high-volume outbound flows. Use osquery with the `process_open_sockets` table to correlate process-to-connection for ransomware staging processes.

Evidence: This is an analysis step that does not directly alter live system state, but volatile evidence relevant to this campaign's double-extortion model must be preserved concurrently: (1) capture RAM from any suspected staging host using WinPmem or DumpIt before any remediation — ransomware encryption keys, exfiltration tool arguments, and C2 channel parameters reside in memory; (2) collect Windows Security Event IDs 4720 (account created), 4732 (added to local group), 4648 (explicit credential use), and 4688 (process creation) filtered on cmd.exe, powershell.exe, wscript.exe, and common ransomware dropper names; (3) capture DNS query logs and proxy/firewall logs for connections to unknown external IPs or domains using DGA-like patterns — double-extortion operators in this campaign exfiltrate to attacker-controlled infrastructure before encrypting; (4) collect VSS (Volume Shadow Copy) status via `vssadmin list shadows` as ransomware families targeting government and education sectors routinely delete shadows as a precursor to encryption.

Eradication — Rotate credentials on any accounts showing anomalous access per D3-CRO (Credential Rotation). Disable or remove unneeded accounts per CIS 5.3 (Disable Dormant Accounts). Enforce MFA on all remote access per CIS 6.4 and on all administrative accounts per CIS 6.5 to close the T1078 valid accounts vector.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 5.3 (Disable Dormant Accounts), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), NIST AC-2 (Account Management), NIST AC-6 (Least Privilege)

Compensating: For teams without an IAM platform: use `net user /domain` and `Get-ADUser -Filter {LastLogonDate -lt (Get-Date).AddDays(-45)} | Disable-ADAccount` to find and disable dormant accounts meeting CIS 5.3 thresholds. Audit local administrator accounts on all hosts via `Get-LocalGroupMember -Group Administrators` and remove non-standard entries. For MFA without enterprise tooling, deploy Duo Free tier or Microsoft Authenticator with Conditional Access on RDP and VPN gateways — both support small deployments at no cost.

Evidence: Credential rotation and account disablement alter live authentication state — capture before acting: (1) export a full Active Directory account list with last logon timestamps (`Get-ADUser -Filter * -Properties LastLogonDate,PasswordLastSet,Enabled`) to establish the pre-rotation baseline and document which accounts showed anomalous access tied to this campaign; (2) collect Windows Security Event ID 4624 Logon Type 3 (network) and Type 10 (remote interactive) logs for all accounts targeted for rotation, covering at minimum 90 days to capture the campaign's likely dwell time across the seven affected organizations; (3) record all currently active sessions (`query session`, `qwinsta /server:`) and authenticated VPN sessions before invalidating tokens, as session artifacts confirm which accounts were actively used by the ransomware operator at time of detection.

Recovery — Validate backup integrity and test restoration procedures before returning affected systems to production. Monitor restored systems with enhanced logging per NIST AU-6 (Audit Record Review, Analysis, and Reporting). Confirm audit log storage capacity is sufficient for extended retention under NIST AU-4 and AU-11.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-4 (Audit Storage Capacity), NIST AU-11 (Audit Record Retention), NIST AU-9 (Protection Of Audit Information)

Compensating: Verify backup integrity without enterprise tooling by computing SHA-256 hashes of backup archives (`certutil -hashfile SHA256`) and comparing against pre-incident hash records to confirm the ransomware operator did not tamper with backups during the exfiltration phase — double-extortion groups in this campaign had sufficient dwell time to identify and corrupt or exfiltrate backup repositories. For enhanced post-recovery monitoring, deploy Sysmon on restored hosts and forward Event IDs 1 (process create), 3 (network connect), 11 (file create), and 13 (registry value set) to a centralized syslog receiver (e.g., rsyslog or Windows Event Forwarding).

Evidence: Before restoring from backup, confirm the backup set predates the intrusion window established during detection analysis — restoring from a compromised backup reintroduces the threat. Specifically: (1) validate backup timestamps against the earliest anomalous Event ID 4624/4648 entry identified in the detection phase; (2) confirm VSS snapshots were not tampered with by checking `vssadmin list shadows` for unexpected deletions correlated with the campaign timeline; (3) after restoration, immediately capture a clean baseline of running processes (`Get-Process`), scheduled tasks (`schtasks /query /fo LIST /v`), and autorun entries (`reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`) to detect any persistence mechanisms the ransomware operator may have implanted prior to the encryption event.

Post-Incident — Conduct a gap assessment against CIS 7.1 (Vulnerability Management Process) and CIS 7.2 (Remediation Process) to identify unpatched systems that may have served as initial access points. Review phishing resilience controls mapped to T1566 and document lessons learned for playbook updates, particularly for sectors matching those targeted in this campaign.

NIST Phase: Post Incident

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

Controls: CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting)

Compensating: Without an enterprise vulnerability scanner, run Microsoft Baseline Security Analyzer or the free Nessus Essentials (up to 16 IPs) against internet-facing assets to identify unpatched RDP, VPN, and web-facing services consistent with the initial access vectors observed in this campaign. For phishing resilience assessment without a commercial platform, send a test phishing simulation using the open-source Gophish framework and review Microsoft 365 or Google Workspace mail delivery logs for macro-enabled attachments and credential-harvesting link clicks that align with T1566 lure patterns used against the education and government sectors in this campaign.

Evidence: Post-incident analysis does not alter live state, but evidence collection for lessons learned must include: (1) the full timeline reconstruction of the double-extortion sequence — initial access timestamp, first lateral movement event, first exfiltration indicator (large outbound transfer logs), and ransomware detonation event — to precisely bound dwell time; (2) any ransomware binary samples or dropper artifacts recovered from quarantine or disk forensics (file paths under `%TEMP%`, `%APPDATA%`, or `C:\ProgramData` are common staging locations for ransomware families targeting this sector profile); (3) indicators of compromise — C2 IP addresses, ransom note filenames, encrypted file extensions, and mutex names — to be shared with sector-specific ISACs (MS-ISAC for government and education, FS-ISAC for financial services) matching the organizations affected in this campaign, consistent with NIST 800-61r3 §4 intelligence-sharing recommendations.

Detection Guidance

No confirmed IOCs are available from source data. Focus detection on behavioral indicators consistent with the mapped MITRE techniques. For T1078 (Valid Accounts): alert on logons outside business hours, logons from new source IPs or countries, and multiple failed logons followed by a success (per NIST AC-7). For T1566 (Phishing): review email gateway logs for high-volume delivery of messages with archive attachments or links to newly registered domains. For T1041 (Exfiltration over C2): baseline outbound data volume per host and alert on deviations exceeding two standard deviations, particularly to unfamiliar external IPs. For T1486 (Data Encrypted for Impact): monitor for rapid, high-volume file rename or modification events, especially involving

common document and database file extensions. Apply D3-SFA (System File Analysis) to detect tampering with system files or configuration changes that precede encryption activity. All detections should be correlated in a SIEM per NIST AU-6. No confirmed hashes, IPs, domains, or file artifacts are available for IOC-based blocking at this time.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1657** — Financial Theft
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel

NIST-800-53R5

- **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
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **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
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

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

SOC2-TSC

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1657	Financial Theft	Impact
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Ransomware.live	https://www.ransomware.live/	T3
Credit Union Cybersecurity Crisis 2025: Strategic Analysis & The ...	https://seceon.com/credit-union-cybersecurity-crisis-2025-strategic...	T3
2023 Top Routinely Exploited Vulnerabilities - CISA	https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-317a	T1
[PDF] Community and Mid-Size Banks Cybersecurity Survey	https://www.joneswalker.com/a/web/3WFqbpX2HQmgjbYp6Y2Rhh/jones-walk...	T3
Cybersecurity Trends from the Top 25 High-Impact Breaches	https://www.youtube.com/watch?v=DirsPcvi0vQ	T3

Generated 2026-06-16 19:19 UTC by TJS Security Command Center