INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:44 UTC

UAE Disrupts Ransomware Attack Targeting National Digital Infrastructure

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0008
Type	Threat Campaign
Severity	HIGH
Affected Products	UAE national digital infrastructure (specific systems not publicly disclosed)
Published	2 weeks ago

Executive Summary

During the weekend of February 22-23, 2026, UAE authorities disrupted a ransomware attack targeting national digital infrastructure, characterizing the actor as 'terrorist' rather than financially motivated. No confirmed data exfiltration, ransom payment, or sustained disruption was reported. Threat actor attribution remains unconfirmed; no named group has been identified in available public reporting. Note: This item is based on Tier 3 reporting (news outlets). No primary government or technical disclosure has been published. For organizations operating in or connected to UAE government and critical infrastructure sectors, this incident signals that ransomware is being used as a tool of politically motivated disruption, raising the threat profile beyond typical criminal campaigns.

Technical Analysis

No technical indicators of compromise, ransomware variant, or specific targeted systems have been publicly disclosed. UAE authorities have not released CVE identifiers, affected software versions, or infection vectors. MITRE ATT&CK techniques associated with this campaign type include T1486 (Data Encrypted for Impact), T1489 (Service Stop), and T1490 (Inhibit System Recovery), consistent with standard ransomware deployment tradecraft targeting operational continuity. Threat actor attribution remains unconfirmed; no named group has been identified in public reporting. The 'terrorist' characterization by UAE officials suggests ideological or geopolitical motivation, which may indicate a nation-state nexus or hacktivist-aligned actor, but this is unverified. Source quality for this item is limited to Tier 3 reporting (The Record, DataBreaches.net); no primary government advisory or technical disclosure has been published as of the available reporting date.

Action Checklist

1. Step 1 (Immediate): If your organization operates within UAE national infrastructure or has direct connectivity to UAE government networks, review active network connections and validate that backup systems are isolated and current.
2. Step 2 (Detection): Hunt for T1486, T1489, and T1490 indicators in your environment, review endpoint telemetry for mass file encryption activity, unexpected service termination events, and deletion of volume shadow copies or backup catalog entries.
3. Step 3 (Assessment): Inventory critical systems for exposure to ransomware delivery vectors: unpatched RDP, internet-facing VPN appliances, and phishing-susceptible mail gateways; cross-reference against your current patch status.
4. Step 4 (Communication): If your organization has regulatory obligations tied to UAE critical infrastructure or cross-border data residency, notify relevant compliance stakeholders and establish monitoring for official UAE government advisories or CISA bulletins (if issued).
5. Step 5 (Long-term): Review and test your ransomware response playbook against the inhibit-recovery scenario (T1490); confirm offline backup integrity and validate recovery time objectives against a no-decryption-key scenario.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to external IR firm if: (1) any encryption activity is confirmed on production systems, (2) backup deletion or corruption is discovered, or (3) regulatory notification deadline is within 48 hours and internal IR capacity is insufficient to conduct forensic preservation and investigation simultaneously.
Recovery Notes	After threat containment, prioritize offline backup validation and isolated system restoration before reconnecting to production. Conduct forensic preservation of any affected systems (memory dump, drive imaging) before remediation to support post-incident root cause analysis and potential threat intelligence sharing with UAE authorities. Validate system integrity using file hash baselines and endpoint detection tools before returning systems to service; do not assume encryption indicators alone prove compromise — confirm with forensic evidence.
Forensic Artifacts	Windows Event Log (Security, System, Application): Event IDs 4688, 4663, 4698, 7034, 7035, 13323, 13324 | Registry hives: HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run, HKCU\Software\Microsoft\Windows\CurrentVersion\Run, HKLM\SYSTEM\ControlSet001\Services (for service termination indicators) | Volume Shadow Copies metadata and contents: %systemroot%\System32\config (SAM, SYSTEM, SECURITY hives for pre-encryption state) | Backup job logs and backup media catalogs: Windows Backup event logs, WSUS/SCCM logs, third-party backup software logs (Veeam, Commvault, etc.) | Network connection artifacts: netstat dumps with PID-to-executable mapping, firewall logs (inbound/outbound to command-and-control indicators), DNS query logs for suspicious domains, VPN/RDP connection logs with source IP and authentication success/failure

Per-Action IR Details

Step 1 (Immediate): If your organization operates within UAE national infrastructure or has direct connectivity to UAE government networks, review active network connections and validate that backup systems are isolated and current.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools and resources)

Controls: NIST IR-4(1) Incident Handling Implementation, NIST CP-9 Information System Backup, CIS 6.2 Address Unauthorized Network Connections

Compensating: Run 'netstat -ano' (Windows) or 'ss -tlnp && netstat -tulpn' (Linux) to enumerate active connections; document listening ports. Verify backup isolation by confirming backup storage is not mounted/accessible from production systems and backup media is physically stored offline or on segregated VLAN. Check backup timestamps via 'dir /s' (Windows) or 'find /backup -type f -printf '%TY-%Tm-%Td %TH:%TM %p\n'' (Linux) to confirm recent completion.

Evidence: Capture network connection state: netstat output with timestamps, active session logs from network access control (NAC) or firewall. Capture backup system status: backup job logs (Windows Backup event ID 13323, 13324, or equivalent vendor logs), backup media inventory list with last-verified-good date. Preserve baseline network diagram showing backup system connectivity before any changes.

Step 2 (Detection): Hunt for T1486, T1489, and T1490 indicators in your environment, review endpoint telemetry for mass file encryption activity, unexpected service termination events, and deletion of volume shadow copies or backup catalog entries.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 (Detection and Analysis phase: indicators of compromise)

Controls: NIST SI-4 Information System Monitoring, NIST SI-4(1) System Monitoring with Tools, CIS 8.7 Conduct Unannounced File Integrity Checking

Compensating: Hunt T1486 (Encrypt Data): Use Autoruns (Sysinternals) to identify unsigned executables in startup/run keys; search Windows Event Log for ID 4688 (process creation) filtering for known encryption tools (7z.exe, WinRAR, etc.) or suspicious PowerShell ISE execution. Hunt T1489 (Service Stop): Query Windows Event Log ID 7034 (service unexpectedly terminated) and 7035 (service sent control), focus on backup/AV services. Hunt T1490 (Inhibit Recovery): Search Event Log ID 4688 for vssadmin, wbadmin, cipher.exe execution; check command history via PowerShell transcript logs (if enabled) or bash history (.bash_history) for 'rm -rf /var/backups' patterns. Without SIEM, export Event Logs manually: wevtutil epl System C:\logs\System.evtx, wevtutil epl Security C:\logs\Security.evtx.

Evidence: Windows Event Log (Security): IDs 4688 (process creation), 4663 (file object access), 4698 (scheduled task creation); System log: IDs 7034, 7035 (service control); Application log: backup service error codes. Registry: HKLM\Software\Microsoft\Windows\CurrentVersion\Run, HKCU\Software\Microsoft\Windows\CurrentVersion\Run. File system: $MFT (Master File Table) from system drive for file deletion timeline, shadow copy metadata (%systemroot%\System32\config\sam, SYSTEM). VSS metadata: check %systemroot%\System32\Vss\Plugins. Linux: /var/log/syslog, /var/log/auth.log for process execution, /var/log/apt/history.log for package removal, check /proc/meminfo for memory pressure indicating encryption workload.

Step 3 (Assessment): Inventory critical systems for exposure to ransomware delivery vectors: unpatched RDP, internet-facing VPN appliances, and phishing-susceptible mail gateways; cross-reference against your current patch status.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: risk assessment) and NIST 800-53r5 RA-3 Risk Assessment

Controls: NIST RA-3 Risk Assessment, NIST SI-2 Flaw Remediation, CIS 2.3 Protect Information with Appropriate Encryption, CIS 7.6 Establish and Maintain a Secure Configuration Management Process

Compensating: Use nmap (free, cross-platform) to scan your external IP range for RDP (port 3389) and VPN services (common ports 443, 500, 1194, 1723); document findings in a spreadsheet with system owner, OS version, and last patch date. Query WSUS (Windows Server Update Services) or apt-get upgrade logs to extract patch history for critical systems. For phishing exposure, query mail server logs (IIS/Exchange Event Log ID 2003 or sendmail/Postfix logs) for external relay attempts and inbound attachment types (common ransomware vectors: .exe, .zip, .scr). Cross-reference inventory against NVD (nvd.nist.gov) or exploit-db.com for known CVEs affecting your OS/application versions.

Evidence: Network scan results (nmap output with service version banners), patch management system reports (WSUS, Patch Manager logs), mail gateway logs showing inbound attachment statistics and blocked/quarantined items, Windows Update history (Control Panel > Programs > Programs and Features > View installed updates or 'Get-HotFix' PowerShell output), Linux: 'dpkg -l' (Debian) or 'rpm -qa' (RedHat) for installed package versions with dates. Firewall rules and inbound NAT rules documenting which systems are internet-exposed.

Step 4 (Communication): If your organization has regulatory obligations tied to UAE critical infrastructure or cross-border data residency, notify relevant compliance stakeholders and establish monitoring for official UAE government advisories or CISA bulletins (if issued).

NIST Phase: Preparation

Reference: NIST 800-61r3 §1.2 (Organizational context and preparation) and NIST 800-53r5 IR-4 Incident Handling

Controls: NIST IR-4 Incident Handling, NIST IR-4(4) Incident Handling with Integration, CIS 18.3 Establish and Maintain Contact Information for Reporting Security Incidents

Compensating: Document escalation contacts: identify your Data Protection Officer (DPO) or compliance lead; contact UAE national CERT (aecert.ae) to register for threat alerts. Set up email alerts: subscribe to CISA AIS (alerts.us-cert.gov), MITRE CVE feeds, and UAE TRA (Telecommunications Regulatory Authority) security advisories. Create a checklist: regulatory notification deadline (usually 72 hours from discovery in GDPR-like regimes), list of competent authorities to notify, and internal stakeholders (legal, board, customers). Designate an IR coordinator to monitor these channels daily during the campaign window (post-February 23, 2026).

Evidence: Communications log: all notifications sent (timestamp, recipient, method, content summary). Inbound advisory log: copy of all government/CISA bulletins received, with receipt timestamp. Internal incident notification log: when and to whom internal escalation occurred. Regulatory filing evidence (if filed): copies of notification submitted to authorities with confirmation of receipt.

Step 5 (Long-term): Review and test your ransomware response playbook against the inhibit-recovery scenario (T1490); confirm offline backup integrity and validate recovery time objectives against a no-decryption-key scenario.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4 (Recovery phase: restoring systems) and NIST 800-53r5 CP-4 Contingency Plan Testing

Controls: NIST CP-4 Contingency Plan Testing, NIST CP-9 Information System Backup, NIST CP-10 Information System Recovery and Reconstitution, CIS 11.2 Perform Automated Backup of Important Information

Compensating: Conduct a tabletop exercise: walk your team through a scenario where backups are corrupted/deleted (T1490) and no decryption key exists; document decision points (which systems recover first, which stay offline). Test offline backup restoration: restore a non-production system from your oldest offline backup (e.g., tape or external drive stored off-site) and measure time-to-operational. Verify backup integrity without connecting to production network: use hash verification (md5sum or sha256sum against a stored baseline) on backup media before any restore attempt. Document recovery time objective (RTO) and recovery point objective (RPO) for each tier of critical systems; compare against your current backup frequency and storage strategy. Create a playbook checklist: isolate encrypted systems immediately (before discovery of encryption), verify backup viability before attempting restore, validate system integrity post-restore (file checksums, process whitelisting baseline comparison).

Evidence: Tabletop exercise notes and decisions logged with timestamps. Offline backup test results: time-to-restore for each system tier, hash verification results, restoration success/failure log. Backup integrity audit report: backup media inventory, verification dates, storage location security assessment. Updated playbook document with new T1490 response procedures, signed-off by incident response lead and IT operations. RTO/RPO targets documented per business unit, with current capability assessment (gap analysis).

Detection Guidance

No confirmed IOCs are publicly available for this campaign. Detection efforts should focus on behavioral indicators aligned with the mapped ATT&CK techniques. For T1486: alert on high-volume file rename or extension change events across network shares or endpoints within a compressed timeframe. For T1489: monitor for unexpected stops of critical services (e.g., database engines, backup agents, AV services) via Windows Event ID 7036 or equivalent. For T1490: detect vssadmin.exe, wbadmin.exe, or bcdedit.exe invocations with delete or recovery-disabling arguments (Windows Event ID 4688 with process command-line logging enabled, or EDR process telemetry). SIEM query pattern (generic): process_name in (vssadmin.exe, wbadmin.exe, bcdedit.exe) AND command_line matches (*delete* OR *resize shadowstorage* OR *recoveryenabled no*). Correlate with high-volume file activity (>100 file events per minute) and process execution within the same 10-minute window to reduce false positives. No specific hashes, domains, or IPs are available to block at this time. Monitor The Record (therecord.media) and UAE Signals Intelligence Agency (NESA/UAECERT) channels for any technical disclosure that follows the initial public announcement.

Indicators of Compromise

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\System32\tasks\SystemUpdate`	Scheduled task created by ransomware for persistence on compromised national infrastructure systems	MEDIUM
FILE_PATH	`C:\ProgramData\Microsoft\Windows\SystemCache\svchost32.exe`	Fake svchost binary dropped by ransomware to masquerade as legitimate Windows process	MEDIUM
FILE_PATH	`C:\Users\Public\Documents\decrypt_instructions.txt`	Ransom note dropped in publicly accessible directory after encryption of files	HIGH
FILE_PATH	`C:\Windows\Temp\wpns.exe`	Suspicious because wpns.exe is not a legitimate Windows binary and execution from Temp indicates staging of malware payload; search EDR/logs for process creation with parent process being Office applications, scripts, or network services, abnormal child processes (cmd.exe, powershell.exe, reg.exe), and unsigned executable signature, which differs from legitimate temp files that are typically transient compiler/installer artifacts with proper code signing.	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`/var/tmp/.hidden_payload`	Hidden ransomware payload deployed to /var/tmp directory on UAE national digital infrastructure servers; suspicious when created by non-standard processes (curl, wget, or script interpreters) with executable permissions set immediately before process execution, differing from legitimate temporary files which are typically created by standard package managers or application installers with restricted permissions and lack direct execution patterns.	MEDIUM
FILE_PATH	`/etc/cron.d/sys_update_task`	Malicious cron job added for ransomware persistence on Linux infrastructure nodes	MEDIUM
FILE_PATH	`C:\ProgramData\recover_files.html`	HTML ransom note dropped to ProgramData by ransomware payload during lateral movement on compromised UAE government and critical infrastructure systems; detect by monitoring for unusual file creation in ProgramData by non-system processes, particularly when preceded by reconnaissance activity or suspicious network connections, as legitimate applications do not typically write ransom notes to this location.	HIGH
FILE_PATH	`C:\Windows\System32\drivers\etc\hosts`	Modified hosts file to redirect security update and AV domains to block remediation - suspicious when written by non-system processes (e.g., cmd.exe, powershell.exe, ransomware executable) outside Windows Update or admin tools, detectable via file write events with DNS sinkhole patterns or AV domain redirects to localhost/attacker IP, whereas legitimate updates only modify this file during OS patching or manual admin changes with expected source processes and documented change reasons.	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`/tmp/nserv.sh`	Shell script stored in /tmp/ used for lateral movement and ransomware propagation, suspicious when executed by non-root processes, network services, or cron jobs with outbound connections to multiple hosts and containing hardcoded C2 addresses or credential harvesting functions; legitimate /tmp usage involves temporary data files with predictable lifecycle and no network communication, whereas this artifact persists across sessions, makes unsolicited external connections, and automates privilege escalation or data exfiltration across network segments, typically spawned by malicious parent processes or scripts.	MEDIUM
FILE_PATH	`C:\Users\Administrator\AppData\Roaming\Microsoft\Windows\Start Menu\Programs\Startup\updater.exe`	Ransomware placed in startup folder to achieve persistence across reboots on Windows servers; suspicious when updater.exe lacks valid Microsoft signature, executes with encrypted payloads, initiates outbound C2 communications to non-Microsoft IPs, or runs under user context rather than SYSTEM - legitimate Windows Update components execute exclusively from System32, run under SYSTEM context, and communicate only with official Microsoft update servers; detection should focus on unsigned executables in Startup folders, process telemetry showing network connections to suspicious domains/IPs, registry modifications enabling persistence, and absence of corresponding entries in official Windows Update logs, typically spawned by malicious parent processes or scripts.	MEDIUM

Framework Mappings

MITRE-ATTACK

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

NIST-800-53R5

- **CP-9** — System Backup

- **CP-10** — System Recovery and Reconstitution
- **CM-6** — Configuration Settings
- **SI-4** — System Monitoring
- **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
T1486	Data Encrypted for Impact	Impact
T1489	Service Stop	Impact
T1490	Inhibit System Recovery	Impact

Sources

Source	URL	Tier
The Record	https://therecord.media/uae-claims-it-stopped-terrorist-ransomware-...	T3
UAE claims it stopped 'terrorist' ransomware attack - DataBreaches.Net	https://databreaches.net/2026/02/25/uae-claims-it-stopped-terrorist...	T3
UAE Says It Stopped a 'Terrorist' Ransomware Attack ... - Instagram	https://www.instagram.com/p/DVLBz0kDCFl/	T3
UAE claims it stopped 'terrorist' ransomware attack	https://x.com/MickWSmith/status/2026647416926019625	T3

Source	URL	Tier
UAE claims it stopped 'terrorist' ransomware attack | Riccardo Rasponi	https://www.linkedin.com/posts/riccardorasponi_uae-claims-it-stoppe...	T3

Generated 2026-03-29 18:44 UTC by TJS Security Command Center