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

Surgeries Canceled, Clinics Closed After University of Mississippi Medical Center Hit by Ransomware Attack

THREAT CAMPAIGN | CRITICAL

SCC Item ID	SCC-CAM-2026-0009
Type	Threat Campaign
Severity	CRITICAL
Affected Products	University of Mississippi Medical Center (UMMC), enterprise IT network and clinical systems
Published	3 weeks ago

Executive Summary

A ransomware attack struck the University of Mississippi Medical Center (UMMC) on approximately February 20, 2026, taking down enterprise IT and clinical systems, forcing outpatient clinic closures and cancellation of non-emergency surgeries for nearly a week. The incident directly disrupted patient care delivery across UMMC's Mississippi facilities, a pattern consistent with healthcare-sector ransomware campaigns that treat operational disruption as leverage. No threat actor has been publicly attributed, and the initial access vector remains undisclosed; healthcare organizations should treat this as an active threat signal for the sector.

Technical Analysis

UMMC sustained a ransomware attack (approximate date: 2026-02-20) that impacted enterprise IT infrastructure and downstream clinical systems, resulting in service-level disruption consistent with MITRE ATT&CK T1486 (Data Encrypted for Impact), T1489 (Service Stop), and T1490 (Inhibit System Recovery). No CVE has been associated with this incident. The applicable weakness category is CWE-693 (Protection Mechanism Failure), reflecting a breakdown in controls that failed to prevent encryption-stage execution. The specific ransomware variant, initial access vector (e.g., phishing, VPN exploitation, exposed RDP, or supply chain), and lateral movement path have not been publicly disclosed as of available reporting. Normal operations were subsequently restored; full forensic details have not been released. Source quality score is 0.64, all confirmed sources are Tier 3 regional and national media. No primary technical disclosure (e.g., CISA advisory, vendor IR report) is available at this time.

Action Checklist

1. Step 1, Immediate: Audit external-facing attack surface, RDP exposure, unpatched VPN appliances, and internet-accessible clinical systems, given undisclosed initial access vector in this incident.
2. Step 2, Detection: Hunt for T1486/T1489/T1490 behavioral indicators in EDR and SIEM: mass file rename/extension change events, Volume Shadow Copy deletion (vssadmin delete shadows), and bulk service termination sequences targeting backup and AV processes.
3. Step 3, Assessment: Verify offline or immutable backup integrity for clinical and administrative systems; confirm backup restoration procedures have been tested within the last 90 days.
4. Step 4, Communication: Brief clinical and operations leadership on current ransomware threat posture for healthcare; confirm downtime procedures and manual fallback workflows are documented and accessible without IT systems.
5. Step 5, Long-term: Review network segmentation between enterprise IT and clinical/OT networks; implement or validate controls aligned with NIST SP 800-53 CP-9 (Information System Backup), SI-3 (Malware Protection), and SC-7 (Boundary Protection). See CISA StopRansomware (https://www.cisa.gov/stopransomware) for updated healthcare-sector TTPs as attribution details for this incident emerge.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm within 2 hours if: (1) initial access vector remains unknown after Step 1 audit, (2) malware persistence indicators (T1547, T1547.1) are discovered during Step 2 hunt, (3) backup integrity validation in Step 3 reveals encryption or corruption of critical backups, or (4) clinical systems remain offline beyond 24 hours post-containment.
Recovery Notes	After threat containment, prioritize restore sequence by clinical criticality: (1) EHR and pharmacy systems first (patient safety and medication management), (2) lab and imaging systems (diagnostic continuity), (3) administrative systems (billing, scheduling). Perform incremental restores from daily backups post-incident, validating data integrity and functional testing after each restore. Maintain parallel manual workflows (paper records, manual order entry) for 48 hours post-restore to catch system failures before full cutover. Document actual recovery time objective (RTO) achieved vs. planned, and update contingency plans with realistic recovery windows.
Forensic Artifacts	Windows Event Logs 4688 (Process Creation), 4689 (Process Termination), 4703 (Service Access) from all affected systems for 72 hours pre-detection | Sysmon Event IDs 1 (ProcessCreate), 2 (FileCreateTime), 3 (NetworkConnect), 10 (ProcessAccess), 11 (FileCreate) from memory or log aggregator | NTFS Master File Table (MFT) and $UsnJrnl from affected volumes showing mass file modification timestamps and extension changes | Network traffic captures (PCAP) from firewall/proxy for 48 hours surrounding attack window showing C2 domains, ports, and data exfiltration patterns | Backup system logs (Veeam, Commvault, or native backup utility) showing backup task execution, integrity checks, and any deletion or corruption events 7 days pre-incident | Endpoint memory dumps (volatility analysis) from initial compromise machine(s) showing injected processes, code caves, and shellcode patterns consistent with ransomware execution

Per-Action IR Details

Step 1, Immediate: Audit external-facing attack surface, RDP exposure, unpatched VPN appliances, and internet-accessible clinical systems, given undisclosed initial access vector in this incident.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation phase: tools, processes, and architecture)

Controls: NIST 800-53 RA-3 (Risk Assessment), NIST 800-53 CA-8 (Penetration Testing), NIST 800-53 SI-4 (Information System Monitoring), CIS 6.1 (Establish network segmentation), CIS 6.2 (Manage internal access)

Compensating: Use Shodan (shodan.io free tier) and Censys (censys.io) to enumerate UMMC's external IP ranges for RDP (3389), VPN ports (500, 1194, 1723), and clinical system ports (80, 443, 8080). Cross-reference with nmap: `nmap -p 3389,500,1194,1723,445 -sV`. For VPN appliance patch status, obtain vendor advisories (Cisco ASA, Palo Alto Networks, Fortinet) from their respective security bulletin pages and validate installed versions against CVE databases. Document all findings in an asset inventory spreadsheet with exposure risk scores.

Evidence: Capture network topology diagrams showing external-to-internal trust boundaries, current firewall ruleset exports (ACLs, NAT rules), VPN appliance configuration files (sanitized of credentials), and external vulnerability scan reports dated pre-incident. Preserve vendor patch baseline documentation to establish pre-breach security posture for post-incident analysis and potential insurance claims.

Step 2, Detection: Hunt for T1486/T1489/T1490 behavioral indicators in EDR and SIEM: mass file rename/extension change events, Volume Shadow Copy deletion (vssadmin delete shadows), and bulk service termination sequences targeting backup and AV processes.

NIST Phase: Detection Analysis

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

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 SI-3 (Malware Protection), NIST 800-53 AU-2 (Audit Events), CIS 8.1 (Collect and analyze logs), CIS 8.2 (Centralize audit logs)

Compensating: Without EDR, use Windows Event Viewer (evt files) and wevtutil command-line: Hunt Windows Event Log 4688 (Process Creation) for vssadmin, wmic, net stop, powershell with bulk rename/delete parameters. Use Sysmon (free, install via GPO) to capture ProcessCreate (Event ID 1) and FileCreateTime (Event ID 2) events to a central log aggregator (rsyslog on Linux, NXLog on Windows). Query for patterns: `vssadmin delete shadows`, `net stop`, `taskkill /F`, and regex file extensions changing to .locked, .encrypted, .crypt, .krypted. Export results to CSV with timestamps and process command lines for timeline reconstruction.

Evidence: Preserve Windows Event Logs 4688, 4689, 4703 (service access), and Sysmon logs (Events 1, 2, 3, 10) from all enterprise systems for the 72 hours pre-detection. Capture file system metadata (MFT, $UsnJrnl from NTFS) showing mass file modifications. Extract $RECYCLE.BIN and unallocated disk sectors for deleted malware binaries. Preserve network traffic captures (PCAP) during the attack window showing C2 communications and lateral movement.

Step 3, Assessment: Verify offline or immutable backup integrity for clinical and administrative systems; confirm backup restoration procedures have been tested within the last 90 days.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (Containment phase: stopping the attack and protecting data)

Controls: NIST 800-53 CP-9 (Information System Backup), NIST 800-53 CP-10 (Information System Recovery and Reconstitution), NIST 800-53 SI-12 (Information Handling and Retention), CIS 3.11 (Protect recovery data)

Compensating: Physically inspect backup storage locations (tape vaults, external hard drives, NAS devices) to confirm they are offline or air-gapped from the network. Use vendor management consoles or command-line tools to validate backup integrity: Veeam (`vbr.exe` backup integrity check), Commvault (CommCell console recovery validation), or rsync/tar checksums for Linux systems. Document last five daily backups with retention dates and cryptographic hash verification (md5sum, sha256sum). Run a full restore test to a sandboxed environment on an isolated network segment; document process time, resource requirements, and success/failure outcomes. Maintain restore procedure documentation accessible offline (printed or on isolated USB).

Evidence: Preserve backup media (tape barcodes, USB serial numbers, NAS serial numbers) with chain-of-custody logs. Document backup software configuration files, encryption key storage locations, and access control lists. Capture

screenshots of backup inventory management systems showing backup dates, sizes, and verification status. Preserve results of the restoration test (logs, timing, resource utilization) to demonstrate recovery capability post-incident.

Step 4, Communication: Brief clinical and operations leadership on current ransomware threat posture for healthcare; confirm downtime procedures and manual fallback workflows are documented and accessible without IT systems.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.3.2 (Preparation: team roles and communication protocols)

Controls: NIST 800-53 CP-2 (Contingency Planning), NIST 800-53 CP-4 (Contingency Plan Testing), NIST 800-53 IR-7 (Incident Response Assistance)

Compensating: Develop and print a one-page clinical downtime reference card in plain language covering: (1) patient registration and triage without EHR (paper forms, manual vital sign recording, specimen labeling by hand); (2) medication dispensing without pharmacy system (manual request to pharmacy with patient ID and dosage); (3) lab order tracking using hardcopy logs with patient ID, order date/time, and expected result time; (4) surgical case postponement and patient notification procedures; (5) emergency contact info for IT, clinical leadership, and external IR firm printed on the card. Distribute laminated copies to nursing stations, lab, OR, and reception. Hold quarterly tabletop drills with clinical and ops staff to practice manual workflows under simulated system outage; document attendance and identified gaps.

Evidence: Preserve all versions of downtime procedures with approval signatures and dates. Document leadership briefing attendance, briefing materials distributed, and any Q&A notes addressing clinical system dependencies. Record tabletop exercise results, gaps identified, and remediation actions with owners and due dates. Capture photos of printed reference materials posted at care delivery points to demonstrate accessibility.

Step 5, Long-term: Review network segmentation between enterprise IT and clinical/OT networks; implement or validate controls aligned with NIST SP 800-53 CP-9 (Information System Backup), SI-3 (Malware Protection), and SC-7 (Boundary Protection). See CISA StopRansomware (https://www.cisa.gov/stopransomware) for updated healthcare-sector TTPs as attribution details for this incident emerge.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities: lessons learned and remediation)

Controls: NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 SI-3 (Malware Protection), NIST 800-53 CP-9 (Information System Backup), NIST 800-53 AC-3 (Access Enforcement), CIS 6.1 (Establish network segmentation), CIS 13.1 (Network architecture)

Compensating: For teams without commercial network segmentation tools (Fortinet, Palo Alto): Implement VLAN-based segmentation using managed switches and open-source firewall (pfsense, OPNsense) positioned at network boundaries. Create three isolated segments: (1) Clinical/OT (EHR, lab systems, imaging, OR control systems) — no outbound internet; (2) Enterprise IT (email, file services, HR systems) — restricted outbound to approved SaaS; (3) Guest/External — fully isolated. Use router ACLs and firewall rules to enforce unidirectional data flow: Clinical systems initiate to Enterprise only for necessary integrations (HL7 messaging, audit logging); Enterprise systems cannot initiate to Clinical. Deploy open-source malware protection: ClamAV antivirus on mail gateway, Snort/Suricata IDS at network boundaries, and Osquery for endpoint visibility (free). Validate backups meet CP-9 requirement: encrypted, tested recovery, offline storage, immutable for 30+ days.

Evidence: Document current and target network topology diagrams with VLAN assignments and firewall rule matrices. Preserve network device configurations (switch VLANs, firewall ACLs, routing policies) with change dates. Capture results of network segmentation testing: ping/traceroute results showing isolation, firewall rule validation, and data flow testing between segments. Preserve malware protection tool deployment logs (antivirus signatures, IDS rule versions, Osquery agent enrollment). Record backup compliance assessment with dates, tool outputs, and remediation timelines.

Detection Guidance

No confirmed IOCs have been publicly released for this incident. Focus detection on behavioral patterns consistent with the mapped MITRE techniques. For T1486: alert on high-velocity file modification events, unexpected file extension changes, and encryption-related process activity (e.g., processes accessing large numbers of files in short windows). For T1489: monitor for service control manager events (Windows Event ID 7036, 7040) showing mass service stops, particularly targeting backup agents, AV services, and database processes. For T1490: alert on execution of 'vssadmin delete shadows', 'wbadmin delete catalog', 'bcdedit /set recoveryenabled no', and equivalent PowerShell equivalents. In SIEM, correlate lateral movement indicators (abnormal SMB traversal, credential reuse across clinical subnets) with encryption-stage activity. CISA's healthcare sector ransomware guidance and the HHS Health Sector Cybersecurity Coordination Center (HC3) threat intelligence portal (https://www.hhs.gov/healthcare-workers-and-professionals/cybersecurity/hhs-health-sector-cybersecurity-coordination-center/index.html) are recommended for updated TTPs as this incident develops.

Indicators of Compromise

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\System32\vssadmin.exe`	Suspicious when vssadmin.exe is executed by non-system processes (cmd.exe, powershell.exe, WMI, or scripts) with "delete shadows" parameters, as attackers use this to destroy volume shadow copies and prevent recovery after ransomware encryption; legitimate administrative use runs directly under SYSTEM context for scheduled maintenance without shadow deletion commands, never spawned from user shells or applications, typically spawned by malicious parent processes or scripts.	HIGH
FILE_PATH	`C:\Windows\System32\wbem\wmic.exe`	wmic.exe spawned by non-system processes (macro, script, or shell) to enumerate system information or disable Windows Defender/backup services; legitimate usage typically originates from System or Administrator-initiated WMI queries, whereas malicious variants execute suspicious WMI namespaces (e.g., Win32_SystemRestore, Win32_Service) without user interaction.	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\System32\bcdedit.exe`	This is suspicious when bcdedit.exe is executed by non-system processes such as Office macros, scripts, rundll32.exe, or command interpreters (cmd.exe, powershell.exe) to disable Windows recovery options, boot configuration data integrity checks, or code integrity enforcement, as legitimate use is restricted to manual administrator execution or Windows Update and never spawned from user applications or scripting engines. Detection should monitor for bcdedit.exe child processes originating from WINWORD.EXE, EXCEL.EXE, cscript.exe, powershell.exe, or rundll32.exe with command-line arguments containing /set, /bootdebug, /recoveryenabled off, or /integrityservices disable, which never occur in legitimate administrative workflows where bcdedit is invoked interactively by administrators from elevated command prompts without parent process ancestry from interpreters or office applications.	HIGH
FILE_PATH	`C:\Windows\System32\cmd.exe`	Command shell spawned by non-system process (e.g., Word, Excel, PowerPoint, or script interpreter) to execute encoded/obfuscated commands or suspicious scripts; legitimate cmd.exe typically invoked by user or system services directly, not by document macros or scripting engines, and legitimate administrative use shows predictable command patterns rather than rapid-fire execution of net, wmic, powershell, or copy commands targeting network shares.	MEDIUM
FILE_PATH	`C:\Windows\System32\net.exe`	Used to enumerate network shares and disable security services when spawned by non-system processes (e.g., cmd.exe, powershell.exe, or Office applications); legitimate use is restricted to interactive administrator sessions or scheduled tasks under SYSTEM context, so look for command-line arguments containing "net share", "net stop", or "net disable-server-auth" paired with parent process anomalies or execution from user-writable directories in EDR/Sysmon logs.	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\System32\taskkill.exe`	Suspicious when taskkill.exe is invoked by non-system processes (macros, scripts, or suspicious parent processes) to terminate security software (defender, antivirus) or database services before ransomware encryption; legitimate use typically originates from System, Administrator console sessions, or known management tools with specific service names, whereas malicious activity shows rapid successive terminations of multiple security/backup services with /f (force) flags and no administrative logging context.	HIGH
FILE_PATH	`C:\Windows\System32\sc.exe`	Suspicious when sc.exe is executed by non-system processes (macro applications, scripts, or unusual parent processes) to disable or stop security services (Windows Defender, backup agents, EDR); legitimate use occurs only when invoked directly by administrators or system processes for service management, whereas malware abuse involves stopping protective services before encryption or lateral movement.	HIGH
FILE_PATH	`C:\Users\Public\`	Common staging directory for ransomware payloads and tools dropped on compromised systems	MEDIUM
FILE_PATH	`C:\ProgramData\`	Used as staging area for ransomware binaries and configuration files when accessed by unusual processes (non-system services) or when executable files are written there by Office macros, scripts, or unsigned binaries; legitimate use is restricted to Windows updates and security software, so monitor for file write events from user applications, cmd.exe, PowerShell, or WMI in this directory combined with subsequent execution from ProgramData or lateral movement attempts.	MEDIUM

Type	Value	Context	Confidence
FILE_PATH	`C:\Windows\Temp\`	Suspicious when executable files are written and immediately executed from C:\Windows\Temp\ by non-system processes (especially Office, scripts, or LOLBins), as legitimate applications rarely stage execution there; hunt for process creation events with parent processes like winword.exe, powershell.exe, or cscript.exe spawning children from this path, or file write events followed by execution within seconds - contrast with normal temp file cleanup and cache operations which occur without subsequent execution chains.	MEDIUM
FILE_PATH	`C:\Windows\System32\wevtutil.exe`	Suspicious when wevtutil.exe is spawned by non-system processes (cmd.exe, powershell.exe, Office macros, or scripting engines) to clear Security, System, or Application event logs, as attackers use this technique post-compromise to destroy forensic evidence; detection should focus on process parent-child relationships showing unsigned or user-context parents, command-line arguments containing "clear-log" or "cl" without corresponding change management tickets, and rapid sequential execution. Legitimate administrative use is typically scheduled through Windows Task Scheduler or Group Policy with documented maintenance windows, executes from System or Administrator contexts, and targets specific retention policies rather than complete log deletion.	HIGH
FILE_PATH	`C:\Windows\System32\cipher.exe`	Suspicious when spawned by non-native processes (PowerShell, WMI, macro applications) or executed from unusual directories, as legitimate cipher.exe usage is rare in typical enterprise environments and the advisory links this to ransomware operations; search EDR/logs for cipher.exe with command-line arguments like /w (wiping free space) or /e (encryption), parent process chains from Office/scripting engines, and execution outside System32 context.	LOW

Type	Value	Context	Confidence
FILE_PATH	`\\UMMC-fileserver\shared\`	Network share path typical of hospital file servers targeted for encryption in healthcare ransomware incidents	LOW
FILE_PATH	`C:\Windows\System32\rundll32.exe`	rundll32.exe execution spawned by Office macros or script interpreters (PowerShell, cmd.exe, WScript) with DLL arguments pointing to temporary directories (%TEMP%, %APPDATA%) or unusual UNC paths, indicating malicious DLL loading; legitimate rundll32.exe typically executes from user-initiated actions with system DLL arguments and parent processes originating from explorer.exe or legitimate applications, not script engines.	MEDIUM
FILE_PATH	`C:\Windows\System32\powershell.exe`	PowerShell execution suspicious when spawned by Office macros, WMI processes, or scheduled tasks with obfuscated command-line arguments (encoded payloads, -EncodedCommand flags, or suspicious module imports like Invoke-WebRequest for credential harvesting); legitimate admin use typically originates from user-initiated console launches or documented automation scripts with readable parameters, whereas ransomware chains show parent process anomalies, network connections to external C2, and rapid lateral movement commands targeting multiple remote systems.	HIGH

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

ISO-27001-2022

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

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
Mississippifreepress	https://www.mississippifreepress.org/university-of-mississippi-medi...	T3
Surgeries canceled, clinics closed after University of Mississippi ...	https://www.djournal.com/news/crime-law-enforcement/surgeries-cance...	T3
UMMC Clinics Remain Closed Nearly a Week After Cyber Attack	https://www.mississippifreepress.org/university-of-mississippi-medi...	T3
Major cyberattack forces closure of clinics across Mississippi - CNN	https://www.cnn.com/2026/02/20/politics/cyberattack-closes-clinics-...	T3
While normal operations have been restored at UMMC, experts say ...	https://www.instagram.com/reel/DVwpE2HCchV/	T3

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