INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-08 13:48 UTC

Healthcare Sector Targeted by New Ransomware Variant "MedLocker"

THREAT CAMPAIGN | **HIGH** | CVSS 9.0

SCC Item ID	SCC-CAM-2026-0426
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.0
Affected Products	Healthcare organizations globally, clinical systems, EHR platforms, operational infrastructure
Published	2026-06-07
Discovery Source	Gemini

Executive Summary

A ransomware campaign targeting healthcare organizations globally is reported to be deploying a variant referred to as 'MedLocker,' encrypting patient data and operational systems while threatening to publish exfiltrated data if ransoms go unpaid, a double-extortion model consistent with established ransomware-as-a-service operations. Clinical systems, electronic health record platforms, and operational infrastructure are reported to be within the campaign's scope. IMPORTANT: The variant name 'MedLocker' and specific technical details originate from secondary, search-grounded sources. No authoritative advisory (CISA, HHS HC3, or confirmed vendor report) has been identified to corroborate this as a named, confirmed variant. Confidence in specific details is LOW pending primary source verification. Organizations should treat this as an elevated threat posture advisory until named sources confirm active targeting.

Technical Analysis

This campaign is reported to follow established ransomware-as-a-service patterns documented against the healthcare sector. The reported attack chain maps to MITRE ATT&CK techniques: initial access via valid accounts (T1078) and phishing (T1566), followed by data encryption for impact (T1486), exfiltration over C2 channel (T1041), financial extortion (T1657), and inhibiting system recovery (T1490). Double-extortion mechanics involve both encryption of local and networked systems and threatened publication of exfiltrated sensitive data. Relevant weaknesses include CWE-311 (missing encryption of sensitive data, exploited to expose data before victim-side encryption), CWE-693 (protection mechanism failure), and CWE-284 (improper access control enabling lateral movement and privilege escalation). No CVE identifier is associated with this

campaign item. No CISA KEV entry exists for this item. CVSS base score is reported at 9.0 (HIGH), treated as an analyst-assigned editorial rating rather than a vendor or NVD score. No confirmed IOCs (hashes, IPs, domains, ransom note signatures) are available from primary sources at this time. All technical specifics should be treated as LOW confidence until corroborated by CISA, HHS HC3, or a vetted vendor threat intelligence report.

Action Checklist

1. Step 1: Containment. Audit and enforce least-privilege access across clinical and EHR systems immediately; disable or restrict accounts showing anomalous authentication patterns consistent with T1078 (valid account abuse). Reference NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Isolate any systems exhibiting unusual encryption activity or high disk I/O from the network pending investigation.
2. Step 2: Detection. Review authentication logs for unusual logon patterns (multiple failed attempts followed by success, off-hours access, impossible travel) per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). Hunt for T1566 phishing delivery artifacts in email gateway logs and T1490 indicators, specifically deletion of Volume Shadow Copies via vssadmin.exe or wmic.exe commands in endpoint logs. No confirmed IOCs are available from primary sources; detection must rely on behavioral patterns until authoritative indicators are published.
3. Step 3: Eradication. Enforce MFA on all externally exposed applications and remote access entry points per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.4 (Require MFA for Remote Network Access). Rotate credentials for any accounts flagged during detection review per D3-CRO (Credential Rotation). Patch operating systems and applications to current supported versions per CIS 7.3 and CIS 7.4 to close unpatched entry points commonly exploited in RaaS initial access. No specific patch or vendor remediation is available for this campaign pending primary source confirmation.
4. Step 4: Recovery. Validate integrity of backup systems before restoration; confirm backups are offline or air-gapped and have not been encrypted or deleted (T1490 directly targets backup infrastructure). Restore from known-good backups only after confirmed eradication of persistence mechanisms. Monitor restored systems for re-encryption activity and anomalous outbound data transfers consistent with T1041 for at least 72 hours post-restoration. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for ongoing log review during recovery.
5. Step 5: Post-Incident. Assess control gaps exposed by this campaign: specifically, gaps in access control (NIST AC-2 Account Management, AC-6 Least Privilege), MFA coverage (CIS 6.3, 6.4, 6.5), and audit logging completeness (NIST AU-2, AU-12). Conduct a tabletop exercise simulating double-extortion ransomware against EHR and clinical systems. If a real incident occurred, engage HHS Office for Civil Rights for HIPAA breach notification assessment; this is an escalation item requiring legal and compliance counsel, not an internal-only determination.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately if any of the following conditions are met: (1) confirmed encryption of EHR patient records or clinical systems constituting a HIPAA breach requiring HHS OCR notification within 60 days and, if >500 individuals affected, media notification — engage legal counsel before any external disclosure; (2) backup infrastructure is found encrypted or deleted, eliminating recovery options and triggering business continuity escalation to executive leadership; (3) evidence of successful data exfiltration (T1041 artifacts, dark web leak site activity) triggering double-extortion notification response; or (4) clinical operations are impaired to the degree that patient safety is at risk, requiring activation of downtime procedures and potential diversion of emergency patients.
Recovery Notes	Restore clinical and EHR systems in priority order: life-safety systems (clinical decision support, medication administration records) first, administrative and billing systems last, and validate each restored system against a known-good configuration baseline before returning to production. Monitor all restored systems for a minimum of 72 hours post-restoration using Sysmon Event ID 11 (FileCreate) scoped to EHR data directories and Wireshark captures filtered on outbound non-RFC1918 traffic, specifically watching for re-encryption activity (mass FileCreate with renamed extensions) and T1041 exfiltration (sustained HTTPS upload to uncategorized external IPs). Do not restore from any backup created within the estimated dwell period — if dwell time cannot be established, default to restoring from the most recent backup predating the first confirmed anomaly by at least 30 days.
Forensic Artifacts	Windows Security Event Log entries for Event ID 4624/4625/4648/4672 on EHR servers and clinical workstations — specifically, logon events for service accounts used by EHR platforms (Epic, Meditech, Cerner) authenticating interactively or from unexpected source IPs, which are not normal operational patterns and indicate T1078 valid account abuse as the lateral movement vector. | Sysmon Event ID 1 (Process Create) logs capturing the full process tree for vssadmin.exe and wmic.exe executions with command-line arguments containing 'delete shadows' or 'shadowcopy delete' — these are the definitive T1490 pre-encryption VSS deletion artifacts that MedLocker-class ransomware executes immediately before the encryption routine begins. | Email gateway logs (O365 Unified Audit Log, on-prem Exchange message tracking, or Proofpoint/Mimecast export) filtered on messages delivered to clinical staff with HTML, ZIP, LNK, or ISO attachments in the 7-day window before first anomaly — preserves T1566 phishing delivery chain evidence and identifies the patient-zero workstation for forensic imaging priority. | File system forensic image of the patient-zero host showing MedLocker ransom note file paths, encrypted file extension pattern, and any dropper or staging binaries in %TEMP%, %APPDATA%\Roaming, or EHR application plugin directories — the ransom note's embedded Bitcoin or Monero wallet address is an intelligence artifact for threat actor tracking and law enforcement referral. | Network flow or Wireshark PCAP data captured at the perimeter firewall or on affected VLAN segments covering the 48-hour window surrounding the encryption event, filtered for large outbound data transfers to non-RFC1918 destinations over HTTPS (port 443) — MedLocker's double-extortion model requires successful exfiltration of patient data before encryption, and this evidence establishes the scope of PHI exposure for HIPAA breach notification analysis.

Per-Action IR Details

Step 1: Containment — Audit and enforce least-privilege access across clinical and EHR systems immediately; disable or restrict accounts showing anomalous authentication patterns consistent with T1078 (valid account abuse). Reference NIST AC-6 (Least Privilege) and CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts). Isolate any systems exhibiting unusual encryption activity or high disk I/O from the network pending investigation.

NIST Phase: Containment

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

Controls: NIST AC-6 (Least Privilege), NIST AC-2 (Account Management), CIS 5.4 (IG1/IG2/IG3) — Restrict Administrator Privileges to Dedicated Administrator Accounts

Compensating: Run the following PowerShell on each suspected EHR host to enumerate accounts with anomalous recent logon times and flag non-dedicated admin accounts actively logged into clinical systems: `Get-WmiObject Win32_NetworkLoginProfile | Select Name,LastLogon,NumberOfLogons | Sort LastLogon -Descending`. Use Sysmon Event ID 1 (Process Create) filtered on high-volume child processes spawned by EHR service accounts (e.g., Epic Hyperspace, Meditech service user) to flag lateral movement. Physically pull network cable or disable switch port for hosts showing sustained high disk I/O (>80% for >5 minutes) if remote isolation is not available.

Evidence: Before isolating: capture a full memory image using WinPMEM or Magnet RAM Capture from any host showing active encryption activity — MedLocker's encryption keys may reside only in volatile memory. Export Windows Security Event Log (Event ID 4624/4625/4648 — logon success/failure/explicit credential use) and Event ID 4672 (special privileges assigned) filtered on EHR service accounts and any accounts authenticating outside business hours or from unexpected source IPs. Preserve current network connections via `netstat -anob > netstat_snapshot.txt` before isolation destroys active C2 channel evidence.

Step 2: Detection — Review authentication logs for unusual logon patterns (multiple failed attempts followed by success, off-hours access, impossible travel) per NIST AU-2 (Event Logging) and CIS 8.2 (Collect Audit Logs). Hunt for T1566 phishing delivery artifacts in email gateway logs and T1490 indicators — specifically, deletion of Volume Shadow Copies via vssadmin.exe or wmic.exe commands in endpoint logs. No confirmed IOCs are available from primary sources; detection must rely on behavioral patterns until authoritative indicators are published.

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 (IG1/IG2/IG3) — Collect Audit Logs

Compensating: Deploy Sysmon with a healthcare-tuned config (SwiftOnSecurity baseline minimum) and hunt for the following without a SIEM: (1) Sysmon Event ID 1 filtering `vssadmin.exe delete shadows` or `wmic shadowcopy delete` — the canonical T1490 VSS deletion signature used by RaaS operators before encryption begins; (2) Sysmon Event ID 11 (FileCreate) for mass creation of files with unusual extensions (e.g., `.medlocked`, `.enc`, or random 6–8 character extensions) in EHR data directories; (3) PowerShell `Get-WinEvent -LogName Security | Where {$_.Id -eq 4625} | Group-Object -Property Message` to surface brute-force patterns against clinical workstation accounts. For email gateway hunting without enterprise tools, export O365 Unified Audit Log or on-prem Exchange message tracking logs and grep for attachments with `.html`, `.zip`, or `.lnk` extensions delivered in the 72-hour window preceding first anomaly.

Evidence: Query email gateway logs for T1566 delivery artifacts: messages with HTML attachments or password-protected archives delivered to clinical staff addresses in the 7 days preceding first anomaly — RaaS initial access frequently uses healthcare-themed lures (patient referral notices, insurance claim attachments). Pull Sysmon Event ID 1 logs for `wmic.exe` and `vssadmin.exe` process executions with parent process chains tracing back to EHR application processes or Office products. Collect Windows PowerShell/Operational Event Log (Event ID 4103/4104 — script block logging) for encoded command execution, which is a common MedLocker-class post-exploitation pattern before the encryption payload is staged.

Step 3: Eradication — Enforce MFA on all externally exposed applications and remote access entry points per CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.4 (Require MFA for Remote Network Access). Rotate credentials for any accounts flagged during detection review per D3-CRO (Credential Rotation). Patch operating systems and applications to current supported versions per CIS 7.3 and CIS 7.4 to close unpatched entry points commonly exploited in RaaS initial access. No specific patch or vendor remediation is available for this campaign item — no mapped control for variant-specific eradication pending primary source confirmation.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 6.3 (IG1/IG2/IG3) — Require MFA for Externally-Exposed Applications, CIS 6.4 (IG1/IG2/IG3) — Require MFA for Remote Network Access, CIS 6.5 (IG1/IG2/IG3) — Require MFA for Administrative Access, CIS 7.3 (IG1/IG2/IG3) — Perform Automated Operating System Patch Management, CIS 7.4 (IG1/IG2/IG3) — Perform Automated Application Patch Management, NIST AC-17 (Remote Access)

Compensating: For MFA enforcement without enterprise IAM budget: enable Windows Hello for Business or configure free RADIUS + Google Authenticator (FreeRADIUS + oath-toolkit) for VPN and RDP entry points within 24 hours. For credential rotation at scale on a 2-person team, use PowerShell `Get-ADUser -Filter * | Set-ADAccountPassword` scoped to the OU containing flagged accounts, forcing reset at next logon. Verify all RDP-exposed clinical workstations have Network Level Authentication (NLA) enforced via GPO: `Computer Configuration > Windows Settings > Security Settings > Local Policies > Security Options > Require NLA`. Scan for residual MedLocker staging artifacts (dropper DLLs in `%TEMP%`, `%APPDATA%`, or EHR application plugin directories) using ClamAV with an updated signature database before returning systems to production.

Evidence: Before credential rotation: export a full snapshot of Active Directory account attributes for flagged accounts using `Get-ADUser -Identity -Properties * | Export-Csv` to preserve evidence of when accounts were last modified, what groups they held, and what logon scripts were attached — MedLocker operators frequently add persistence via group membership changes or logon script modification. Check scheduled tasks on affected hosts (`schtasks /query /fo LIST /v > schtasks_dump.txt`) and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run registry keys for persistence mechanisms installed prior to encryption, which must be confirmed removed before eradication is declared complete.

Step 4: Recovery — Validate integrity of backup systems before restoration; confirm backups are offline or air-gapped and have not been encrypted or deleted (T1490 directly targets backup infrastructure). Restore from known-good backups only after confirmed eradication of persistence mechanisms. Monitor restored systems for re-encryption activity and anomalous outbound data transfers consistent with T1041 for at least 72 hours post-restoration. Reference NIST AU-6 (Audit Record Review, Analysis, and Reporting) for ongoing log review during recovery.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-11 (Audit Record Retention), CIS 3.4 (IG1/IG2/IG3) — Enforce Data Retention

Compensating: Verify backup integrity before restoration by hashing backup files with `Get-FileHash -Algorithm SHA256` and comparing against stored checksums — if no prior hashes exist, treat all backups created within 14 days of first anomaly as potentially compromised and validate against the oldest available offline copy. Deploy Sysmon on restored systems immediately post-restoration and run a Wireshark capture on the restored host's network interface for the first 4 hours, filtering for outbound connections on uncommon ports or to non-RFC1918 destinations — T1041 data exfiltration over standard protocols (HTTPS on port 443 to uncategorized IPs) is the double-extortion data exfiltration mechanism. Monitor Windows Security Event ID 4663 (object access — file encryption writes) on EHR data directories using a targeted audit policy scoped to sensitive patient data paths.

Evidence: Before restoring from backup: document the exact encrypted file extension pattern left by MedLocker on affected systems (e.g., enumerate via `Get-ChildItem -Recurse -Filter *.* | Where {$_.Extension -notin $knownExtensions}`) to establish a forensic baseline of encryption scope for HIPAA breach notification scope assessment. Preserve the ransom note dropped by MedLocker (typically placed in each encrypted directory and on the desktop) as an artifact — its filename, content, and Bitcoin/Monero wallet address are intelligence artifacts useful for threat actor attribution and law enforcement referral. Capture and retain VSS metadata (`vssadmin list shadows`) to document what shadow copies existed and confirm deletion, establishing evidence of intentional data destruction relevant to HIPAA breach analysis.

Step 5: Post-Incident — Assess control gaps exposed by this campaign: specifically, gaps in access control (NIST AC-2 Account Management, AC-6 Least Privilege), MFA coverage (CIS 6.3, 6.4, 6.5), and audit logging

completeness (NIST AU-2, AU-12). Conduct a tabletop exercise simulating double-extortion ransomware against EHR and clinical systems. If a real incident occurred, engage HHS Office for Civil Rights for HIPAA breach notification assessment — this is an escalation item requiring legal and compliance counsel, not an internal-only determination.

NIST Phase: Post Incident

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

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), CIS 6.3 (IG1/IG2/IG3) — Require MFA for Externally-Exposed Applications, CIS 6.4 (IG1/IG2/IG3) — Require MFA for Remote Network Access, CIS 6.5 (IG1/IG2/IG3) — Require MFA for Administrative Access, CIS 7.1 (IG1/IG2/IG3) — Establish and Maintain a Vulnerability Management Process, CIS 7.2 (IG1/IG2/IG3) — Establish and Maintain a Remediation Process

Compensating: Structure the tabletop exercise specifically around MedLocker's double-extortion model: inject a scenario where backup systems are found encrypted mid-recovery and a threat actor publishes a sample of patient records to a dark web leak site 48 hours into the incident — this forces the team to rehearse the HIPAA breach notification decision tree under operational pressure, not just the technical response. Document lessons learned using the NIST 800-61r3 §4 after-action format: what happened, root cause, what worked, what didn't, and specific control improvements with owners and deadlines. Share sanitized TTPs (T1078, T1566, T1490, T1041) with H-ISAC (Health Information Sharing and Analysis Center) to contribute to sector-wide threat intelligence without disclosing PHI.

Evidence: Compile the complete forensic timeline from initial phishing delivery through encryption event for the after-action report: map each attacker action to a log source and timestamp to identify detection gaps — specifically, measure the dwell time between initial T1078 account compromise and first T1490 VSS deletion event, as this gap represents the detection improvement opportunity. Retain all forensic images, log exports, ransom notes, and network captures for a minimum of 6 years per HIPAA retention requirements (45 CFR §164.530(j)) and in compliance with any law enforcement preservation hold if the incident was reported to FBI or CISA.

Detection Guidance

No confirmed IOCs (file hashes, C2 IPs, domains, or ransom note signatures) are available from primary sources for this campaign. Detection must rely on behavioral and heuristic indicators consistent with the mapped MITRE techniques. Key detection priorities: (1) T1078, monitor for successful authentications after repeated failures, off-hours privileged account activity, and accounts accessing EHR or clinical systems outside normal patterns; log sources: Active Directory/identity provider authentication logs, SIEM correlation rules per NIST AU-6. (2) T1566, review email gateway logs for suspicious attachment types (.iso, .lnk, macro-enabled Office files) and URLs delivered to healthcare staff; cross-reference with endpoint execution logs. (3) T1486, alert on mass file rename operations, high-volume encryption activity, or the creation of ransom note files (common naming: README.txt, DECRYPT_INSTRUCTIONS.txt) on file servers and workstations; monitor via EDR behavioral rules. (4) T1490, detect deletion of shadow copies via vssadmin delete shadows or wmic shadowcopy delete commands in Windows event logs (Event ID 4688 with command-line logging enabled). (5) T1041, alert on anomalous outbound data volumes, especially to unknown external IPs or cloud storage endpoints, prior to encryption onset; monitor via network flow data and proxy logs per CIS 8.2. Recommended D3FEND countermeasures: D3-LAM (Local Account Monitoring) for credential abuse detection, D3-SFA (System File Analysis) for ransomware artifact detection, D3-MFA (Multi-factor Authentication) to reduce T1078 effectiveness.

Framework Mappings

MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1486** — Data Encrypted for Impact
- **T1041** — Exfiltration Over C2 Channel
- **T1657** — Financial Theft
- **T1490** — Inhibit System Recovery

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
- **AC-3** — Access Enforcement
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1486	Data Encrypted for Impact	Impact
T1041	Exfiltration Over C2 Channel	Exfiltration
T1657	Financial Theft	Impact
T1490	Inhibit System Recovery	Impact

Sources

Source	URL	Tier
Healthcare Cybersecurity Challenges & Threats - 2026 | Rubrik	https://www.rubrik.com/insights/healthcare-cybersecurity-challenges...	T3
The U.S. health system vulnerabilities - PMC - NIH	https://pmc.ncbi.nlm.nih.gov/articles/PMC12781349/	T1
Cybersecurity risks in healthcare are an ongoing crisis - IBM	https://www.ibm.com/think/insights/cybersecurity-in-healthcare-ongi...	T3
Vulnerability to Cyberattacks and Sociotechnical Solutions for ...	https://www.jmir.org/2024/1/e46904/	T3
Exploitable Vulnerabilities That Expose Healthcare Facilities Surged ...	https://health-isac.org/2023-state-of-cybersecurity-for-medical-dev...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-06-08 13:48 UTC by TJS Security Command Center