INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:33 UTC

Ransomware Campaigns Disrupt U.S. Healthcare and Municipal Government Operations, March 2026

THREAT CAMPAIGN | **CRITICAL**

SCC Item ID	SCC-CAM-2026-0104
Type	Threat Campaign
Severity	CRITICAL
Affected Products	U.S. healthcare system (unspecified); U.S. city government (unspecified); broader healthcare and state/local government sectors
Published	2026-03-26
Discovery Source	Gemini

Executive Summary

In March 2026, ransomware attacks struck at least one U.S. healthcare system and one U.S. city government, forcing clinic shutdowns, patient care delays exceeding one week, and a municipal state of emergency. Both sectors carry high ransomware risk due to legacy infrastructure, limited patching velocity, and reliance on credential-based remote access. Organizations in healthcare and state/local government should treat this activity as a signal to validate controls now, not after an incident. Note: specific incident details are sourced from Gemini (search-augmented) and have not been independently corroborated by CISA or primary government advisories as of this analysis.

Technical Analysis

No specific CVEs, ransomware variant names, or confirmed threat actors have been attributed to these incidents in available source data. Attack precursors are consistent with well-documented ransomware initial access patterns mapped to MITRE ATT&CK: phishing (T1566), exploitation of public-facing applications against unpatched systems (T1190), and valid account abuse via weak or reused credentials (T1078). Post-access activity likely follows standard ransomware execution chains: lateral movement via remote services (T1021), file discovery (T1083), service disruption (T1489), inhibit system recovery (T1490), and data encryption (T1486). Relevant CWEs include CWE-521 (weak password requirements), CWE-522 (insufficiently protected credentials), CWE-693 (protection mechanism failure), and CWE-1188 (insecure default initialization). No CVSS scores are available; no CISA KEV entries are associated with these specific incidents. CVSS and EPSS scores are 0.0 reflecting absence of a discrete CVE, not low severity. Qualitative severity is rated critical based on

operational impact to life-safety infrastructure.

Action Checklist

1. Step 1, Immediate: Audit and enforce MFA on all remote access entry points (VPN, RDP, Citrix, web-based portals); disable or isolate accounts with weak or reused passwords identified via credential scanning.
2. Step 2, Immediate: Verify backup integrity and confirm offline or immutable backup copies exist for critical systems; test restoration procedures if not validated within the last 30 days.
3. Step 3, Detection: Search endpoint and network logs for T1566 phishing delivery artifacts, T1078 anomalous authentication (off-hours logins, new geolocations, credential stuffing patterns), and T1021 lateral movement via RDP or SMB.
4. Step 4, Assessment: Inventory internet-facing systems and cross-reference against current patch status; prioritize unpatched systems with known exploitation history via CISA KEV catalog and sector-specific advisories (CISA Healthcare, CISA SLTT guidelines).
5. Step 5, Communication: Brief leadership on ransomware exposure posture; confirm incident response retainer and playbooks are current, contacts are validated, and tabletop exercises are scheduled if not completed in the past 12 months.
6. Step 6, Long-term: Implement or validate network segmentation between clinical/operational systems and administrative networks; review acceptable-use and phishing-awareness training completion rates.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm and legal immediately if any Step 3 detection search (phishing artifacts, anomalous authentication, lateral movement) yields positive hits with evidence of data exfiltration, encryption activity, or active compromise within the past 7 days.
Recovery Notes	Post-containment recovery sequence: (1) validate ransomware was fully removed via clean backup restoration to isolated network, confirm no persistence via reinfection attempt within 48 hours of restoration; (2) restore systems in order of criticality (EHR/clinical, then administrative, then lower-priority); (3) re-enable MFA and force password reset for all accounts post-recovery, monitor Event Log 4625 (failed logins) for 14 days to detect any attacker re-entry attempts using old credentials; (4) conduct forensic analysis of encrypted files, ransom note, and infection vector before reintroducing systems to production network.

Forensic Artifacts	Windows Security Event Log (Event IDs 4624, 4625, 4688, 4720, 4722, 4769 [Kerberos ticket requests]) — minimum 30 days retention | Windows System Event Log (Event ID 7034 [service crashed], 7045 [service installed]) — persistence mechanisms | Filesystem Master File Table (MFT) and USN Journal ($Extend\$UsnJrnl) — file modification timeline and encryption activity | Prefetch files (C:\Windows\Prefetch*.pf) and ShimCache (registry HKLM\SYSTEM\CurrentControlSet\Services\bam\State\UserSettings) — execution timeline and malware utility launches | Network flow logs (NetFlow, syslog, firewall logs) — source/dest IP/port pairs, lateral movement via RDP/SMB, C2 communications | Mail gateway logs with message headers, attachment details, delivery timestamps — phishing infection vector | Browser download history (Chrome/Edge SQLite databases, Firefox profile) — malware delivery mechanism | Registry hives (HKLM\Software, HKCU\Software) — persistence keys (Run, RunOnce, Scheduled Tasks), RDP usage tracking (RecentServers) | DNS query logs — suspicious domain resolutions (newly registered, .onion, known C2 domains)

Per-Action IR Details

Step 1 — Immediate: Audit and enforce MFA on all remote access entry points (VPN, RDP, Citrix, web-based portals); disable or isolate accounts with weak or reused passwords identified via credential scanning.

NIST Phase: Preparation

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

Controls: NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-4 (Identifier Management), CIS 6.2 (Enforce MFA for all accounts), CIS 6.3 (Require MFA for remote access)

Compensating: Use Windows Active Directory built-in MFA via Windows Hello for Business, or deploy free RADIUS-based MFA (e.g., FreeRADIUS + Google Authenticator). For credential scanning: run Invoke-ADPasswordQualityCheck (PowerShell, free) or manually audit AD users with 'Password Never Expires' flag set; export via dsquery user | dsget user -pwdneverexpires. Cross-reference against breach databases via pwned.com API (batch, free tier available).

Evidence: Capture baseline before changes: (1) Active Directory user object export with LastLogon, pwdLastSet, userAccountControl attributes; (2) VPN/RDP authentication logs (Windows Event Log 4624, 4625 for account logons); (3) failed authentication attempts from the past 30 days; (4) current MFA enrollment status per access portal. Store in read-only archive before disabling any accounts.

Step 2 — Immediate: Verify backup integrity and confirm offline or immutable backup copies exist for critical systems; test restoration procedures if not validated within the last 30 days.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1.2 (Tools and resources: backup and recovery validation)

Controls: NIST 800-53 CP-9 (Information System Backup), NIST 800-53 CP-10 (Information System Recovery and Reconstitution), CIS 3.11 (Backup and recovery procedures)

Compensating: For resource-constrained orgs: document backup location and media type (tape, external drive, cloud bucket) manually; verify offline status by confirming backups are on air-gapped media or in cloud with write-once-read-many (WORM) enabled (AWS S3 Object Lock, Azure immutable blob storage—both free tier eligible for small backup sets). Test recovery via restore-to-staging: select one database per critical system, document restore time, compare data integrity (row count, checksum) before/after. Use free tools: rsync verification scripts or tar + sha256sum for filesystem backups.

Evidence: Before any backup test: (1) capture current backup media inventory (location, encryption status, WORM settings); (2) cryptographic hash of backup catalogs (e.g., sha256sum of backup database index); (3) recovery procedure documentation with last-validated date; (4) screenshots of cloud immutability settings if applicable. Store hashes separately from production for forensic validation post-incident.

Step 3 — Detection: Search endpoint and network logs for T1566 phishing delivery artifacts, T1078 anomalous authentication (off-hours logins, new geolocations, credential stuffing patterns), and T1021 lateral movement via RDP or SMB.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.3 (Analysis: log review and data correlation)

Controls: NIST 800-53 SI-4 (Information System Monitoring), NIST 800-53 AU-12 (Audit Generation), CIS 8.2 (Log all authentication attempts), CIS 8.5 (Log DNS queries)

Compensating: Without SIEM: (1) T1566 phishing: export mail gateway logs (if available) to CSV; grep for suspicious file extensions (.exe, .zip, .scr, .ps1) and external sender domains; cross-reference against known phishing indicators via public IP reputation lists (e.g., Spamhaus ZEN free API). (2) T1078 anomalous auth: export Windows Event Log 4624/4625 via wevtutil.exe qe Security '/q:*[System[(EventID=4624 or EventID=4625)]]' > auth.csv; pivot on LogonType 10 (RDP) and 3 (network), group by source IP, identify IPs with 20 failed attempts in 1-hour window. (3) T1021 lateral movement: monitor SMB traffic via netstat -ano for port 445 and RDP (3389) connections; parse Windows Event Log 4688 (process creation) for 'net.exe use', 'psexec', 'wmic' commands; correlate with failed 4625 events.

Evidence: Preserve immediately: (1) Windows Security Event Log (Event IDs 4624, 4625, 4688, 4720, 4722) with 7+ days retention if available; (2) mail gateway logs with message metadata (sender, subject, attachment names, delivery timestamps); (3) network flow data (NetFlow, syslog from firewalls) showing source/dest IP, port, protocol for all RDP/SMB traffic; (4) endpoint EDR telemetry if available (process chains for suspicious utilities); (5) DNS query logs for suspicious domain resolutions (*.onion, newly registered domains, known C2 domains per OSINT feeds).

Step 4 — Assessment: Inventory internet-facing systems and cross-reference against current patch status; prioritize unpatched systems with known exploitation history in healthcare and government sectors per CISA KEV catalog.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: tools and asset inventory)

Controls: NIST 800-53 CM-2 (Baseline Configuration), NIST 800-53 SI-2 (Flaw Remediation), CIS 7.1 (Maintain inventory of all software), CIS 7.3 (Address unauthorized software)

Compensating: Manual inventory: use nmap (free, open-source) to port-scan all known networks; document services on ports 443, 80, 3389, 22, 445, 139 with banner grabbing (nmap -sV). Cross-reference software versions against CISA KEV (publicly available CSV at https://www.cisa.gov/known-exploited-vulnerabilities-catalog, free). For Windows: query via PowerShell Get-HotFix | Export-Csv patches.csv per system; compare against CISA KEV CVE list. For Linux: rpm -qa or dpkg -l > installed_packages.txt; cross-check critical packages (Apache, OpenSSH, etc.) against KEV. Prioritize systems running unpatched versions of: Exchange (common in healthcare), RDP services, VPN appliances, web-facing file share applications.

Evidence: Preserve baseline before patching: (1) complete software inventory with version numbers and build dates; (2) patch deployment log showing which patches were applied and when (Windows Update history, /var/log/yum.log for Linux); (3) documented current patch level per system vs. CISA KEV baseline; (4) network topology diagram showing which systems are internet-facing vs. internal; (5) firewall rules and WAF configurations currently protecting these systems.

Step 5 — Communication: Brief leadership on ransomware exposure posture; confirm incident response retainer and playbooks are current, contacts are validated, and tabletop exercises are scheduled if not completed in the past 12 months.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.3 (Mitigation strategies and incident handling: communication plan)

Controls: NIST 800-53 IR-1 (Incident Response Policy), NIST 800-53 IR-4 (Incident Handling), CIS 19.1 (Incident response plan)

Compensating: Create lightweight incident response playbook (template-based): document 5-7 key scenarios (ransomware, data exfiltration, credential compromise, supply chain event, insider threat); for each, define: (1)

detection trigger (specific log/alert pattern), (2) first responder action (who to notify, what to preserve), (3) escalation ladder (tier-1 team → security manager → CISO → legal), (4) communication protocol (internal vs. external notification template). Validate contact list: phone numbers, email, out-of-office backup for each tier. Schedule tabletop via free tools: calendar invite with scenario deck (no-cost, in-house facilitation). Confirm 3rd-party retainer details: scope of services, response time SLA, cost-sharing for forensic imaging.

Evidence: Capture before briefing: (1) current incident response plan with last-reviewed date and signoff; (2) contact roster with phone/email per escalation tier; (3) evidence preservation procedures (chain of custody template, forensic imaging tooling list); (4) communication templates for internal notification, customer notification, regulatory notification; (5) tabletop exercise results (if conducted within 12 months) and lessons-learned log.

Step 6 — Long-term: Implement or validate network segmentation between clinical/operational systems and administrative networks; review acceptable-use and phishing-awareness training completion rates.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (Preparation: tools and risk assessment)

Controls: NIST 800-53 AC-4 (Information Flow Enforcement), NIST 800-53 SC-7 (Boundary Protection), NIST 800-53 AT-2 (Security Awareness and Training), CIS 1.4 (Network segmentation), CIS 14.2 (Security training)

Compensating: Network segmentation without enterprise firewall: use VLAN tagging on managed switches (document VLAN assignment); implement Windows Firewall Group Policy on each client/server to block traffic from admin network to clinical network (netsh advfirewall firewall add rule name='Block Clinical Access' dir=in action=block remoteip= protocol=tcp); document firewall rules and test with ping/telnet to verify isolation. Training tracking: export Active Directory user list; cross-reference against LMS (learning management system) completion reports or create manual tracking spreadsheet (user → completion date → module version); target 100% by 90 days. Use free training resources: CISA phishing training modules, SANS Cyber Aces (phishing awareness), internal scenario simulations.

Evidence: Before implementing segmentation: (1) network topology diagram showing current data flows between clinical and admin systems; (2) list of clinical systems (medical devices, EHR databases, imaging servers) and admin systems (file servers, email, HR) with IP ranges; (3) Windows Firewall policy baseline and group policy audit logs showing failed inter-segment traffic; (4) screenshot of training LMS enrollment and completion rates per user/department; (5) documentation of any business-critical cross-segment traffic that must be whitelisted (e.g., billing system querying EHR—this requires proxy or approved rule).

Detection Guidance

No confirmed IOCs are available for these specific incidents. Detection should focus on behavioral indicators consistent with the identified MITRE techniques. For T1566 (phishing): review email gateway logs for high-volume inbound campaigns, lookalike domains, and macro-enabled attachments. For T1078 (valid accounts): alert on authentication anomalies, failed logins followed by success, logins from unexpected geographies or ASNs, and service account activity outside normal hours. For T1021 (remote services): flag new or unusual RDP, SMB, or WMI lateral movement between workstations, especially from non-admin endpoints. For T1490 and T1489 (recovery inhibition, service stop): monitor for Volume Shadow Copy deletion commands (vssadmin delete shadows), bulk file modification events across shared drives, and unexpected service stop/disable actions via Windows Event IDs 7036 and 7040. For T1486 (data encryption): watch for high-rate file rename events with unfamiliar extensions on file servers. SIEM correlation rules should chain these behavioral indicators rather than relying on single-event triggers. Cross-reference any detections against CISA's StopRansomware advisories for current variant-specific indicators.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`none confirmed`	No IOCs have been confirmed for these specific incidents in available source data. This field will be updated if primary-source attribution becomes available.	LOW

Framework Mappings

MITRE-ATTACK

- **T1190** — Exploit Public-Facing Application
- **T1490** — Inhibit System Recovery
- **T1078** — Valid Accounts
- **T1021** — Remote Services
- **T1486** — Data Encrypted for Impact
- **T1566** — Phishing
- **T1489** — Service Stop
- **T1083** — File and Directory Discovery

NIST-800-53R5

- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **CM-7** — Least Functionality
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **CM-6** — Configuration Settings

- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **5.2**
- **6.3** — Require MFA for Externally-Exposed Applications
- **7.3** — Perform Automated Operating System Patch Management
- **7.4** — Perform Automated Application Patch Management
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(i)** — Security Awareness and Training

NIST-CSF-2

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

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.8.8** — Management of technical vulnerabilities
- **A.5.34** — Privacy and protection of personal information

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1190	Exploit Public-Facing Application	Initial-Access
T1490	Inhibit System Recovery	Impact
T1078	Valid Accounts	Defense-Evasion
T1021	Remote Services	Lateral-Movement
T1486	Data Encrypted for Impact	Impact
T1566	Phishing	Initial-Access
T1489	Service Stop	Impact

Technique ID	Technique Name	Tactic
T1083	File and Directory Discovery	Discovery

Sources

Source	URL	Tier
The U.S. health system vulnerabilities - PMC - NIH	https://pmc.ncbi.nlm.nih.gov/articles/PMC12781349/	T1
The U.S. health system vulnerabilities	https://pubmed.ncbi.nlm.nih.gov/41345652/	T1
Red Team Realities: Defending Hospitals to City Halls	https://www.youtube.com/watch?v=zTk2nXIw2ts	T3
Public Sector Cybersecurity | Why State & Local ...	https://www.sentinelone.com/blog/why-the-public-sector-under-attack...	T3
4 Threats to Cybersecurity for State and Local Governments	https://rampxchange.com/blog/4-threats-to-cybersecurity-for-state-a...	T3

Generated 2026-03-29 18:33 UTC by TJS Security Command Center