INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-18 14:11 UTC

INC Ransomware's Sector-Targeting Strategy Keeps Healthcare in the Crosshairs

THREAT CAMPAIGN | **CRITICAL** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0507
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	7.5
Affected Products	Healthcare sector organizations (hospitals, health systems, medical providers, no specific vendor products identified)
Published	2026-06-17T15:46:25
Discovery Source	Rss

Executive Summary

INC ransomware operators are actively targeting healthcare organizations by exploiting weak authentication controls and inadequate credential protection, forcing operational shutdowns that directly threaten patient care. The group has maintained sustained attack campaigns against hospitals and health systems since mid-2023, prioritizing sectors where downtime creates life-safety pressure to pay quickly. Organizations that have not hardened remote access, enforced multi-factor authentication, and audited privileged credentials face elevated risk of a disruptive, high-cost ransomware incident.

Technical Analysis

INC ransomware is a human-operated ransomware group active since mid-2023, targeting healthcare and critical infrastructure through authentication weaknesses (CWE-287: Improper Authentication) and inadequate credential protection (CWE-522: Insufficiently Protected Credentials). Primary entry vectors include exploitation of external-facing remote services (T1133), abuse of valid accounts (T1078), Remote Desktop Protocol lateral movement (T1021.001), and phishing (T1566). Credential access is achieved through brute force (T1110). Post-access, operators execute service disruption (T1489), inhibit system recovery (T1490), and deploy file encryption (T1486). No specific CVE is associated with this campaign; the group exploits configuration weaknesses and authentication gaps rather than novel unpatched vulnerabilities. No vendor-specific patch exists; remediation requires authentication hardening, credential hygiene, and access control enforcement.

Action Checklist

1. Step 1: Containment. Audit and restrict all externally exposed remote access services (RDP, VPN, remote desktop gateways). Disable any accounts with default, shared, or unchanged credentials immediately. Enforce network segmentation to isolate clinical systems from administrative and internet-facing infrastructure. Reference: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement).
2. Step 2: Detection. Review authentication logs for brute-force patterns (repeated failed logins followed by success, especially on RDP or VPN endpoints) mapped to MITRE T1110 and T1078. Query SIEM for T1133 indicators: external remote service authentication events outside business hours or from unexpected geographies. Enable and centralize audit logs from all remote access points per CIS 8.2 (Collect Detailed Audit Logs). Alert on T1489 indicators: mass service stop commands, VSS deletion (vssadmin delete shadows), and volume shadow copy removal consistent with T1490.
3. Step 3: Eradication. Enforce MFA on all externally exposed services, administrative accounts, and remote access paths (CIS 6.3, CIS 6.4, CIS 6.5; NIST IA controls). Rotate credentials for all privileged accounts and service accounts, prioritizing those with remote access (D3-CRO: Credential Rotation). Remove or disable dormant accounts per CIS 5.3. Enforce least-privilege access per NIST AC-6 to limit lateral movement potential. Configure account lockout policies per NIST AC-7 to block brute-force entry.
4. Step 4: Recovery. Validate that all backup systems are offline or immutable and test restoration from a known-clean backup prior to resuming full operations. Confirm VSS and backup integrity were not tampered with (T1490). Monitor endpoint and network telemetry for re-encryption activity or re-establishment of unauthorized remote sessions post-remediation. Validate MFA enforcement is active on all remote access paths before reconnecting isolated systems.
5. Step 5: Post-Incident. Conduct a privileged access review to identify all accounts that had unnecessary remote access rights. Map gaps to NIST AC-5 (Separation of Duties) and AC-6 (Least Privilege). Implement a formal vulnerability management process per CIS 7.1 and 7.2 to catch authentication configuration drift. Develop or update an IR playbook specifically for ransomware scenarios targeting clinical systems, including pre-authorized isolation decisions to compress defender response time.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to organizational leadership, legal counsel, and the HHS Office for Civil Rights breach notification process if any system containing electronic Protected Health Information (ePHI) was encrypted or accessed by INC operators, or if clinical operations (EHR access, medical devices, or patient care workflows) are disrupted — both conditions trigger mandatory HIPAA Breach Notification Rule timelines and may constitute a life-safety emergency requiring activation of downtime procedures.

Recovery Notes	Before restoring any clinical system to production, perform a full malware scan using an offline boot environment (e.g., Windows Defender Offline or a live Linux distro with ClamAV) against restored volumes to confirm the INC encryptor and any dropped persistence mechanisms (scheduled tasks, registry run keys, or backdoor binaries in `C:\ProgramData\` or `C:\Windows\Temp\`) have been eliminated. After reconnection, maintain elevated monitoring on all RDP and VPN authentication events for a minimum of 30 days — INC operators have demonstrated persistence in healthcare environments and may retain access through secondary credential sets or pre-positioned remote access tools not discovered during initial eradication. Validate clinical application integrity (EHR database checksums, medical device configuration files) in coordination with clinical engineering before allowing patient care workflows to resume on restored systems.
Forensic Artifacts	Windows Security Event Log (Event IDs 4624 Type 10, 4625, 4648, 4672) from all RDP-exposed and domain controller hosts — the INC brute-force pattern produces a high-density cluster of 4625 events from a single source IP followed by a solitary 4624 Type 10 success, establishing the initial access timestamp and originating IP for the intrusion timeline | VSS and shadow copy state evidence: `vssadmin list shadows` output (or its absence), Windows Backup operational log (Event IDs 4098/4099), and Prefetch files for `VSSADMIN.EXE` and `WMIC.EXE` at `C:\Windows\Prefetch\` — INC's pre-encryption routine deletes all shadow copies, and Prefetch timestamps record the exact execution time of this anti-recovery step | INC ransom note files named `INC-README.txt` dropped in every encrypted directory — their filesystem creation timestamps (captured via `$MFT` parsing using a tool such as MFTECmd) establish the precise moment encryption began on each volume and support sequencing of the attack timeline across multiple hosts | Windows System Event Log (Event IDs 7036 and 7034) documenting mass service termination events — INC's encryptor kills database engines (SQL Server, MySQL), backup agents, and security software services immediately before beginning encryption, and this log sequence is a high-confidence behavioral indicator distinguishing INC from other ransomware families | VPN and remote desktop gateway authentication logs covering the 72-hour window preceding the first confirmed encryption event — INC operators typically conduct credential testing and low-and-slow reconnaissance via VPN or RDP days before deploying the encryptor, and these logs establish the full dwell time for breach notification scope assessment and potential HIPAA regulatory reporting

Per-Action IR Details

Step 1: Containment — Audit and restrict all externally exposed remote access services (RDP, VPN, remote desktop gateways). Disable any accounts with default, shared, or unchanged credentials immediately. Enforce network segmentation to isolate clinical systems from administrative and internet-facing infrastructure. Reference: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement).

NIST Phase: Containment

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

Controls: NIST AC-17 (Remote Access), NIST AC-3 (Access Enforcement), NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Run `netstat -ano | findstr :3389` and `Get-NetTCPConnection -LocalPort 3389` on each Windows host to enumerate active RDP listeners. Use Windows Firewall (`netsh advfirewall firewall add rule name='Block RDP' protocol=TCP dir=in localport=3389 action=block`) to block inbound RDP at the host level immediately. For VPN gateways without centralized management, pull the active session table from the gateway admin console and terminate sessions from unexpected source IPs. Segment clinical VLANs by applying ACLs on managed switches using the switch CLI to drop inter-VLAN routing between clinical and administrative subnets.

Evidence: Before disabling any accounts or terminating sessions, capture: (1) a full dump of active RDP and VPN sessions including source IP, username, session start time, and session ID from the remote access gateway logs; (2) `Get-NetTCPConnection` output and `query session /server:` on each exposed host to document all live authenticated sessions; (3) Windows Security Event Log Event ID 4624 (Logon Success) and 4625 (Logon Failure) entries from RDP-exposed hosts covering the prior 72 hours — INC operators typically conduct credential brute-force reconnaissance 24-48 hours before deploying the encryptor; (4) VPN authentication logs including the full session table from the concentrator — preserve these before any account disablement destroys the association between compromised credential and session.

Step 2: Detection — Review authentication logs for brute-force patterns (repeated failed logins followed by success, especially on RDP or VPN endpoints) mapped to MITRE T1110 and T1078. Query SIEM for T1133 indicators: external remote service authentication events outside business hours or from unexpected geographies. Enable and collect audit logs per CIS 8.2 across all remote access points. Alert on T1489 indicators: mass service stop commands, VSS deletion (vssadmin delete shadows), and volume shadow copy removal consistent with T1490.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis

Controls: NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-12 (Audit Record Generation), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, use PowerShell on each RDP-exposed Windows host to query failed logon events: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4625} | Select-Object TimeCreated, @{n='TargetUser';e={$_.Properties[5].Value}}, @{n='SourceIP';e={$_.Properties[19].Value}} | Export-Csv C:\IR\rdp_failures.csv`. Follow with a correlated query for Event ID 4624 (Type 10 = RemoteInteractive) from the same source IPs to identify successful logins after failure bursts. For VSS tampering detection, run `Get-WmiObject Win32_ShadowCopy` on all servers — zero results on a production server is a high-confidence indicator INC has already executed its pre-encryption cleanup. Deploy a Sigma rule for `vssadmin delete shadows` and `wmic shadowcopy delete` process creation events (Event ID 4688) using `Get-WinEvent` filtering on ProcessCommandLine if Sysmon is not yet deployed; install Sysmon with the SwiftOnSecurity config immediately to capture Event ID 1 (Process Create) going forward.

Evidence: Capture before any containment action that would flush logs or terminate sessions: (1) Windows Security Event Log exports (Event IDs 4624, 4625, 4648, 4672) from all RDP and VPN-adjacent hosts — INC operators leave a characteristic pattern of high-volume 4625 events from a single source IP followed by a solitary 4624 Type 10 event marking credential success; (2) `vssadmin list shadows` output and WMI query `Get-WmiObject Win32_ShadowCopy` — absence of shadow copies on a host with previously configured backups is forensic evidence of INC pre-encryption activity (T1490); (3) Windows System Event Log for Event ID 7036 (Service stopped) and 7034 (Service crashed unexpectedly) — INC's encryptor systematically stops database, backup, and AV services before encrypting; (4) Prefetch files at `C:\Windows\Prefetch\` for `VSSADMIN.EXE-*.pf`, `WMIC.EXE-*.pf`, and the INC encryptor binary prefetch entry, which persist after process termination and provide execution timestamps.

Step 3: Eradication — Enforce MFA on all externally exposed services, administrative accounts, and remote access paths (CIS 6.3, CIS 6.4, CIS 6.5; NIST IA controls). Rotate credentials for all privileged accounts and service accounts, prioritizing those with remote access (D3-CRO: Credential Rotation). Remove or disable dormant accounts per CIS 5.3. Enforce least-privilege access per NIST AC-6 to limit lateral movement potential. Configure account lockout policies per NIST AC-7 to block brute-force entry.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-6 (Least Privilege), NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For MFA enforcement without an enterprise IAM platform, implement Windows Hello for Business or free RADIUS-based MFA (FreeRADIUS + Google Authenticator PAM module) in front of VPN endpoints. For RDP, enforce Network Level Authentication (NLA) via Group Policy (`Computer Configuration > Administrative Templates > Windows Components > Remote Desktop Services > Require NLA`) as a compensating barrier — NLA forces credential validation before session establishment, reducing exposure of the Windows login surface. For credential rotation on a 2-person team, prioritize in this order: (1) all accounts with Event ID 4624 Type 10 logins in the compromise window, (2) all Domain Admin and local Administrator accounts, (3) all service accounts with interactive logon rights. Use `net user /domain` and `Get-ADUser -Filter {Enabled -eq $true -and LastLogonDate -lt (Get-Date).AddDays(-45)}` to enumerate and disable dormant accounts.

Evidence: Before rotating any credentials or modifying accounts, capture: (1) a complete Active Directory user export including LastLogonDate, PasswordLastSet, and group memberships — `Get-ADUser -Filter * -Properties LastLogonDate,PasswordLastSet,MemberOf | Export-Csv C:\IR\ad_users.csv` — this documents the pre-incident privilege state for forensic and regulatory purposes; (2) a dump of all currently active authenticated sessions across domain controllers using `Get-ADDomainController -Filter * | ForEach {query session /server:$_.Name}` — rotating credentials while an adversary holds a live Kerberos TGT does not invalidate the existing ticket without also purging the LSASS session; (3) memory acquisition (via WinPmem or Magnet RAM Capture) from any host suspected of adversary presence BEFORE credential rotation, as INC operators may cache credentials in LSASS memory for lateral movement and this evidence is destroyed on session termination or reboot.

Step 4: Recovery — Validate that all backup systems are offline or immutable and test restoration from a known-clean backup prior to resuming full operations. Confirm VSS and backup integrity were not tampered with (T1490). Monitor endpoint and network telemetry for re-encryption activity or re-establishment of unauthorized remote sessions post-remediation. Validate MFA enforcement is active on all remote access paths before reconnecting isolated systems.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Before reconnecting any restored system, verify backup integrity by comparing file hash manifests: generate SHA-256 hashes of restored critical system files against a known-good baseline using `Get-FileHash -Algorithm SHA256 -Path C:\Windows\System32\*.exe | Export-Csv C:\IR\hash_baseline.csv`. Deploy a YARA rule scanning for known INC ransomware encryptor signatures (INC drops a ransom note named `INC-README.txt` — scan all volumes with `yara64.exe inc_rule.yar C:\ -r` before reconnecting). For re-encryption monitoring without EDR, configure Sysmon Event ID 11 (FileCreate) alerts on bulk `.INC` extension file creation as a tripwire, combined with a scheduled task running `Get-NetTCPConnection` every 5 minutes and alerting on new outbound connections to non-whitelisted IPs on ports 443, 3389, or 4443.

Evidence: Before reconnecting isolated systems to the production network, capture and preserve: (1) a file system timeline from restored hosts using `dir /t:w /s C:\ > C:\IR\file_timeline_post_restore.txt` to establish a clean post-recovery baseline for future comparison; (2) confirmation of VSS state via `vssadmin list shadows` and Windows Backup event logs (Event IDs 4098, 4099 in the Microsoft-Windows-Backup operational log) to document that shadow copies were re-created after the INC attack and are intact; (3) netflow or firewall logs covering the full recovery window, preserved to an offline location, to support detection of any C2 re-establishment — INC operators have been observed attempting to re-access environments via secondary backdoors after initial remediation.

Step 5: Post-Incident — Conduct a privileged access review to identify all accounts that had unnecessary remote access rights. Map gaps to NIST AC-5 (Separation of Duties) and AC-6 (Least Privilege). Implement a formal vulnerability management process per CIS 7.1 and 7.2 to catch authentication configuration drift. Develop or update an IR playbook specifically for ransomware scenarios targeting clinical systems, including pre-authorized isolation decisions to compress defender response time.

NIST Phase: Post Incident

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

Controls: NIST AC-5 (Separation Of Duties), NIST AC-6 (Least Privilege), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For privileged access review without a PAM platform, export all Active Directory group memberships for Domain Admins, Remote Desktop Users, and VPN user groups: `Get-ADGroupMember -Identity 'Domain Admins' -Recursive | Export-Csv C:\IR\da_members.csv`. Cross-reference against HR termination records and last logon dates to identify orphaned or excessive accounts. For authentication configuration drift detection, schedule a monthly automated check using a PowerShell script that validates account lockout policy (`Get-ADDefaultDomainPasswordPolicy`), MFA registration completeness (via IdP API or manual audit), and RDP exposure (`Test-NetConnection -ComputerName -Port 3389` from an external IP) — output to a shared log reviewed in a standing security meeting. For the ransomware-specific IR playbook, document pre-authorized clinical system isolation thresholds (e.g., 'if >3 hosts show bulk file extension changes to .INC within a 5-minute window, the on-call administrator is pre-authorized to isolate the affected VLAN without additional approval') to eliminate the approval latency that INC exploits in healthcare environments.

Evidence: Preserve and archive for lessons-learned and potential regulatory response: (1) the complete incident timeline reconstructed from Windows Security Event Logs, VPN authentication logs, and firewall netflow, covering the initial brute-force attempts through encryptor execution — this is the primary artifact for HIPAA Breach Notification Rule assessment if PHI was on encrypted systems; (2) the pre-incident AD export and post-incident account audit comparison to document the privilege reduction actions taken; (3) all INC ransom note instances (`INC-README.txt`) found on affected file systems — these establish the attribution to INC ransomware for law enforcement referral and cyber insurance claims; (4) a documented after-action report mapping the attack path (initial access via weak RDP/VPN credentials → lateral movement → VSS deletion → encryption) to the specific control gaps identified, to satisfy HIPAA Security Rule §164.308(a)(8) (Evaluation) requirements for documented security reviews following a security incident.

Detection Guidance

Focus detection on the four primary techniques INC operators use for initial access and lateral movement. For T1110 (Brute Force) and T1078 (Valid Accounts): query authentication logs for accounts with 5 or more consecutive failed logins followed by a successful login within a 10-minute window, especially on RDP (Event ID 4625 then 4624 on Windows), VPN gateway logs, and Citrix access logs. For T1133 (External Remote Services): alert on successful VPN or RDP authentications originating from IP ranges with no prior organizational history or from anonymization infrastructure (Tor exit nodes, commercial VPN ranges). For T1021.001 (RDP Lateral Movement): correlate successful RDP sessions (Event ID 4624 logon type 10) that chain across multiple internal hosts in short succession; this pattern indicates post-compromise lateral movement. For T1489 and T1490 (Service Stop and Inhibit Recovery): alert on bulk service termination events, execution of vssadmin.exe delete shadows, wbadmin.exe delete catalog, or bcdedit.exe /set recoveryenabled no. These commands appearing in process creation logs (Event ID 4688 or Sysmon Event ID 1) are high-fidelity ransomware pre-deployment indicators. Cross-reference all detections against CIS 8.2 audit log coverage gaps; if remote access logs are not centralized in your SIEM, this kill chain is effectively blind.

Framework Mappings

MITRE-ATTACK

- **T1021.001** — Remote Desktop Protocol
- **T1133** — External Remote Services

- **T1078** — Valid Accounts
- **T1566** — Phishing
- **T1110** — Brute Force
- **T1489** — Service Stop
- **T1490** — Inhibit System Recovery
- **T1486** — Data Encrypted for Impact

NIST-800-53R5

- **AC-17** — Remote Access
- **AC-20** — Use of External Systems
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-8** — Spam Protection
- **AC-7** — Unsuccessful Logon Attempts
- **CM-6** — Configuration Settings
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-4** — Incident Handling

OWASP-TOP10-2021

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

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.2** — Use Unique Passwords
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

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

NIST-CSF-2

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1133	External Remote Services	Persistence
T1078	Valid Accounts	Defense-Evasion
T1566	Phishing	Initial-Access
T1110	Brute Force	Credential-Access
T1489	Service Stop	Impact
T1490	Inhibit System Recovery	Impact
T1486	Data Encrypted for Impact	Impact

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/inc-ransomwa...	T3
Security vulnerabilities in healthcare: an analysis of medical devices ...	https://pmc.ncbi.nlm.nih.gov/articles/PMC10758361/	T1
[PDF] Medtech Vulnerability Communications Toolkit	https://healthsectorcouncil.org/wp-content/uploads/2023/10/MVCT-202...	T3
Cybersecurity - FDA	https://www.fda.gov/medical-devices/digital-health-center-excellenc...	T1

Source	URL	Tier
85% of healthcare IT leaders say passwordless access is a priority ...	https://www.facebook.com/duosec/posts/85-of-healthcare-it-leaders-s...	T3

Generated 2026-06-18 14:11 UTC by TJS Security Command Center