INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-26 13:29 UTC

Beast Ransomware Group Claims Attack on Canadian Dental Practice Lessard Dental

THREAT CAMPAIGN | HIGH | CVSS 8.1

SCC Item ID	SCC-CAM-2026-0224
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	8.1
Affected Products	Lessard Dental (Canadian family dental practice), patient data reportedly at risk
Published	2026-04-25
Discovery Source	Gemini

Executive Summary

The Beast ransomware group has claimed responsibility for an attack on Lessard Dental, a Canadian family dental practice, threatening to publish sensitive patient health information unless a ransom is paid. The attack follows a double-extortion model: data was exfiltrated before or during encryption, meaning the threat persists even if systems are restored. For healthcare and dental organizations, this incident signals continued targeting of small and mid-size practices that hold high-value patient data but carry limited security resources.

Technical Analysis

Beast ransomware has claimed a double-extortion attack against Lessard Dental. No CVE is associated with this incident. The initial access vector has not been publicly confirmed. MITRE ATT&CK techniques mapped to this campaign include: T1078 (Valid Accounts, likely initial access), T1041 (Exfiltration Over C2 Channel), T1657 (Financial Theft), and T1486 (Data Encrypted for Impact). The double-extortion model involves exfiltration prior to or concurrent with encryption, with threatened public data release as secondary leverage. Attribution is based solely on the Beast group's own claim; independent technical verification from primary threat intelligence platforms or law enforcement has not been confirmed in available open sources. All corroborating sources are T3 tier (community threat intelligence feeds and social media). No IOCs, ransom note samples, or technical indicators have been published in available open sources at this time. PHI is the presumed target data class given the practice type.

Action Checklist

1. Step 1: Containment. If you operate a dental or healthcare practice on shared infrastructure or use similar practice management software, immediately audit remote access points (VPN, RDP, patient portals) for unauthorized sessions. Disable any unrecognized active sessions and rotate credentials for all administrative accounts.
2. Step 2: Detection. Review authentication logs for anomalous Valid Account usage (T1078): off-hours logins, logins from unfamiliar IPs, or privilege escalation on accounts tied to practice management or billing systems. Monitor for large outbound data transfers that could indicate exfiltration (T1041). No confirmed IOCs are publicly available for this specific incident; monitor threat intelligence feeds for Beast group indicators as they emerge.
3. Step 3: Eradication. Initial access vector is unconfirmed. As a precaution, audit all internet-facing services (VPN concentrators, remote desktop, patient portals, email gateways) for misconfigurations or unpatched software. Enforce MFA on all remote access and administrative accounts. Review third-party vendor access to practice management systems.
4. Step 4: Recovery. Verify backup integrity and confirm backups are stored offline or in an air-gapped location inaccessible from the primary network. Before restoring any systems, validate that persistence mechanisms (scheduled tasks, startup entries, unauthorized user accounts) have been removed. Post-remediation, monitor for re-intrusion attempts targeting the same access vectors.
5. Step 5: Post-Incident. This incident exposes common control gaps in small healthcare practices: absence of MFA on remote access, insufficient network segmentation, limited endpoint detection capability, and no tested incident response plan. Map identified gaps to NIST CSF 2.0 Protect and Detect functions and NIST SP 800-66 Rev. 1 (HIPAA Security Rule guidance for healthcare). Conduct a tabletop exercise simulating ransomware double-extortion to validate response readiness.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal counsel and privacy officer if any evidence confirms PHI exfiltration — Canadian PIPEDA and applicable provincial health privacy legislation (Alberta HIA, Ontario PHIPA, Quebec Law 25) impose mandatory breach notification obligations to regulators and affected patients, and the double-extortion model means data exposure risk persists independently of whether ransom is paid or systems are restored.
Recovery Notes	Before restoring any practice management system (Dentrix, Eaglesoft, or equivalent), validate that the backup predates the earliest evidence of Beast group dwell time — not just the encryption event — as ransomware operators typically maintain access for days to weeks before deploying the encryptor, meaning recent backups may contain attacker-planted persistence. Post-restoration, maintain elevated monitoring on all RDP, VPN, and patient portal authentication logs for a minimum of 30 days, specifically watching for T1078 (Valid Account) reuse from the same source IPs or accounts identified during investigation. Confirm with your practice management software vendor that application-level audit logs are intact and have not been tampered with, as these logs are required for both regulatory breach assessment and insurance claim substantiation.

Forensic Artifacts	Practice management software audit logs (Dentrix: C:\Dentrix\Data\AuditLog or SQL Server audit tables; Eaglesoft: SQL Server dbo.AuditLog table) — these record all admin-level data access, exports, and patient record queries that would reveal the scope of PHI accessed or staged for exfiltration by Beast operators during dwell time. | Windows Security Event Log Event ID 4663 (Object Access — file read/copy) on the server hosting patient records or the practice management database, filtered for bulk sequential access to patient record files or database exports (.bak, .mdf, .csv) which would indicate data staging prior to exfiltration. | Firewall and router logs showing large outbound HTTPS transfers (port 443) or connections to cloud storage domains (Mega.nz, pCloud, or anonymous file-sharing services) from practice management or file servers in the 7–14 days preceding encryption — Beast group commonly uses legitimate cloud services to blend exfiltration traffic. | VSS deletion artifacts: Windows System Event Log Event ID 8224 (VSS service stopped) and PowerShell ScriptBlock logs (Event ID 4104) or Process Creation logs (Sysmon Event ID 1) showing execution of `vssadmin`, `wmic shadowcopy`, or `bcdedit /set recoveryenabled no` — these are near-universal ransomware pre-encryption preparation steps and establish timeline. | Ransom note files dropped by Beast encryptor (typically named README.txt, BEAST_README.txt, or similar, deposited in every encrypted directory) — preserve full filesystem paths and creation timestamps via `forfiles /S /M *README* /C "cmd /c echo @path @fdate @ftime"` to reconstruct the encryption propagation timeline and confirm which systems were fully encrypted versus partially affected.

Per-Action IR Details

Step 1: Containment — If you operate a dental or healthcare practice on shared infrastructure or use similar practice management software, immediately audit remote access points (VPN, RDP, patient portals) for unauthorized sessions. Disable any unrecognized active sessions and rotate credentials for all administrative accounts.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy (RS.MA-01: Execute IR plan, categorize, contain, communicate, mitigate)

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST IA-5 (Authenticator Management), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.2 (Establish an Access Revoking Process), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Export active RDP sessions via PowerShell: `Get-RDUserSession` on Windows Server or query `netstat -ano | findstr :3389` to enumerate established RDP connections, then cross-reference PIDs with `tasklist /FI "PID eq "`. For VPN, pull active session logs from your concentrator's admin console (e.g., Fortinet FortiGate: `get vpn ssl monitor`; SonicWall: Active Sessions page). Kill unrecognized sessions immediately. Rotate all admin passwords using a local password manager (Bitwarden free tier) and document all rotated accounts in a shared incident log.

Evidence: BEFORE disabling sessions, capture forensic snapshots: export Windows Security Event Log Event ID 4624 (Logon Type 10 = RemoteInteractive/RDP, Type 3 = Network) and 4625 (failed logons) filtered to the 72-hour window prior to discovery. Export VPN gateway logs showing source IP, session duration, bytes transferred, and authenticated username for all sessions in the same window. Screenshot or export active session lists from practice management software (e.g., Dentrix, Eaglesoft, Curve Dental) admin consoles before terminating. Preserve these logs to an offline USB or write-protected network share before any credential rotation.

Step 2: Detection — Review authentication logs for anomalous Valid Account usage (T1078): off-hours logins, logins from unfamiliar IPs, or privilege escalation on accounts tied to practice management or billing systems. Monitor for large outbound data transfers that could indicate exfiltration (T1041). No confirmed IOCs are publicly available for this specific incident; monitor threat intelligence feeds for Beast group indicators as they emerge.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis (DE.AE-02: Analyze adverse events; DE.AE-03: Correlate information from multiple sources; DE.AE-07: Integrate CTI into analysis)

Controls: NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM, run this PowerShell one-liner to extract suspicious logon events: `Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.TimeCreated -gt (Get-Date).AddDays(-7)} | Select-Object TimeCreated, @{n='User';e={$_.Properties[5].Value}}, @{n='IP';e={$_.Properties[18].Value}}, @{n='LogonType';e={$_.Properties[8].Value}} | Export-Csv C:\IR\logons.csv`. For exfiltration detection, use Wireshark or Windows Firewall logs (`C:\Windows\System32\LogFiles\Firewall\pfirewall.log`) to identify large outbound flows to non-practice IPs on ports 443, 80, or uncommon ephemeral ports. Install Sysmon (SwiftOnSecurity config) to capture process creation (Event ID 1) and network connections (Event ID 3) going forward. Monitor RANSOMWATCH or the Beast group's known dark web leak site for Lessard Dental data postings.

Evidence: Pull Windows Security Event Log for Event ID 4672 (Special Privilege Logon — indicates admin-level rights assigned at logon) and 4728/4732/4756 (user added to privileged group) for all accounts associated with Dentrix, Eaglesoft, or equivalent practice management software service accounts. Export DNS query logs (Windows DNS debug log at `%SystemRoot%\System32\dns\dns.log` if enabled, or router/firewall DNS logs) for queries to Tor exit nodes, Mega.nz, or file-sharing domains (common Beast exfiltration staging). Capture firewall/router netflow or connection logs showing total bytes-out per destination IP in the 7 days preceding discovery — Beast ransomware operators typically stage exfiltration over multiple sessions before deploying the encryptor.

Step 3: Eradication — Initial access vector is unconfirmed. As a precaution, audit all internet-facing services (VPN concentrators, remote desktop, patient portals, email gateways) for misconfigurations or unpatched software. Enforce MFA on all remote access and administrative accounts. Review third-party vendor access to practice management systems.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication (RS.MA-01: Remove threat from environment, verify eradication)

Controls: NIST SI-2 (Flaw Remediation), NIST CM-7 (Least Functionality), NIST IA-2 (Identification and Authentication — Organizational Users), NIST SA-9 (External System Services), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Run a free vulnerability scan using OpenVAS (Greenbone Community Edition) or Microsoft Baseline Security Analyzer against all internet-facing systems. For third-party vendor access review, export all accounts from your practice management software (Dentrix: Admin > Security > User Management; Eaglesoft: Setup > Security) and compare against a current vendor list — disable any accounts for vendors not actively under contract. Use `net localgroup administrators` and `net user` on each Windows host to enumerate local admin accounts. Enable MFA on all remote access using free tiers of Duo Security or Microsoft Authenticator paired with your existing VPN or RDP gateway. Document all changes in a dated incident log.

Evidence: Before removing any persistence mechanisms, image or export: Windows Scheduled Tasks (`schtasks /query /fo LIST /v > C:\IR\tasks.txt`), Windows Services (`sc query type= all state= all > C:\IR\services.txt`), and registry Run keys (`reg export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run C:\IR\run_keys.reg`). Collect the full user account list including last logon timestamps (`net user > C:\IR\users.txt`). For practice management servers, export the application's own audit log showing all admin-level actions in the 30 days prior to discovery — Beast operators frequently create backdoor local accounts or add existing accounts to admin groups during dwell time to maintain persistence after initial access.

Step 4: Recovery — Verify backup integrity and confirm backups are stored offline or in an air-gapped location inaccessible from the primary network. Before restoring any systems, validate that persistence mechanisms (scheduled tasks, startup entries, unauthorized user accounts) have been removed. Post-remediation, monitor for re-intrusion attempts targeting the same access vectors.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery (RC: Execute recovery plan, restore systems, verify integrity, communicate)

Controls: NIST IR-4 (Incident Handling), NIST CP-9 (System Backup), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Verify backup integrity by restoring a single non-production test file from your most recent backup set before committing to full restoration — Beast ransomware operators are known to target backup systems during dwell time to maximize leverage. Use `CertUtil -hashfile SHA256` to compare hash values of restored files against known-good pre-incident hashes if available. Post-restoration, deploy Sysmon with Event ID 3 (Network Connection) logging enabled and pipe logs to a free ELK stack or simply monitor `C:\Windows\System32\winevt\Logs\Microsoft-Windows-Sysmon%4Operational.evtx` for new outbound connections to previously unseen IPs. Set a Windows Task Scheduler alert or cron job to run `netstat -ano` every 15 minutes and log output for the first 30 days post-recovery.

Evidence: Before initiating any restoration, collect and preserve: VSS (Volume Shadow Copy) status (`vssadmin list shadows`) — Beast and similar ransomware routinely delete shadow copies using `vssadmin delete shadows /all /quiet` or `wmic shadowcopy delete`; absence of shadow copies is itself a forensic indicator of ransomware activity. Capture the Master Boot Record (`dd if=/dev/sda of=/mnt/evidence/mbr.img bs=512 count=1` on Linux, or FTK Imager on Windows) from any encrypted or suspect system before reimaging. Export Windows System Event Log for Event ID 7045 (new service installed) and 7036 (service state change) which may reveal ransomware dropper services. Preserve encrypted file samples with ransom note (do not delete) for potential future decryption if Beast group keys are later released or law enforcement recovers them.

Step 5: Post-Incident — This incident exposes common control gaps in small healthcare practices: absence of MFA on remote access, insufficient network segmentation, limited endpoint detection capability, and no tested incident response plan. Map identified gaps to NIST CSF 2.0 Protect and Detect functions and NIST SP 800-66r2 (HIPAA Security Rule guidance for healthcare). Conduct a tabletop exercise simulating ransomware double-extortion to validate response readiness.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity (GV, ID: Lessons learned, update policies, improve detection, share intelligence)

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-2 (Incident Response Training), NIST IR-3 (Incident Response Testing), NIST RA-3 (Risk Assessment), NIST SI-5 (Security Alerts, Advisories, and Directives), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Conduct a 2-hour tabletop using the CISA Ransomware Readiness Assessment (RRA) free tool — scenario-inject Beast's double-extortion model specifically: at the 45-minute mark, reveal that patient PHI was exfiltrated before encryption to test the team's breach notification decision process under Canada's PIPEDA breach reporting requirements and applicable provincial health privacy law (e.g., Alberta HIA, Ontario PHIPA). Document lessons learned in a structured format referencing NIST 800-61r3 §4 and file findings against each NIST CSF 2.0 Protect/Detect subcategory. Use the free CISA Cyber Hygiene (CyHy) scanning service for ongoing external attack surface monitoring at no cost.

Evidence: For the lessons-learned report, compile and retain: the complete incident timeline reconstructed from preserved logs (Windows Security, VPN, practice management audit logs); a copy of the Beast group's leak site claim (screenshot with timestamp and URL) preserved as evidence of extortion; any ransom note files recovered from encrypted systems (preserve original filenames and directory paths); and a data inventory of what PHI categories were potentially exfiltrated (patient names, DOBs, treatment records, insurance data) to support mandatory breach notification assessment under PIPEDA and provincial health privacy legislation. This documentation package is required for regulatory reporting and should be treated as legal-hold material.

Detection Guidance

No confirmed IOCs for this incident are available in open sources at time of writing. Detection should focus on behavioral indicators consistent with Beast ransomware TTPs and the mapped MITRE techniques. Key detection signals: (1) T1078, authentication events for accounts logging in outside normal hours or from unexpected geographic locations; failed login spikes followed by successful authentication; (2) T1041, anomalous outbound transfer volumes on practice management servers or file servers, particularly to unfamiliar external IPs; (3) T1486, rapid file rename events or mass file extension changes on shared drives, which may indicate active encryption; (4) T1657, unauthorized access to financial records or billing systems. Log sources to prioritize: Windows Security Event Log (Event IDs 4624, 4625, 4648, 4672), VPN and remote access authentication logs, DNS query logs for unusual external destinations, and endpoint process creation logs for ransomware staging activity. Monitor threat intelligence platforms and industry-specific information sharing and analysis centers (ISAC) feeds for Beast group IOCs as this incident develops.

Framework Mappings

MITRE-ATTACK

- **T1041** — Exfiltration Over C2 Channel
- **T1657** — Financial Theft
- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **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
- **IR-4** — Incident Handling
- **SC-13** — Cryptographic Protection

NIST-CSF-2

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

HIPAA-SECURITY

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

ISO-27001-2022

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

- **A.5.34** — Privacy and protection of personal information
- **A.8.24** — Use of cryptography

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1041	Exfiltration Over C2 Channel	Exfiltration
T1657	Financial Theft	Impact
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion

Sources

Source	URL	Tier
Beast Ransomware Group Targets Canadian Clinic Lessard Dental	https://www.dexpose.io/beast-ransomware-group-targets-canadian-clin...	T3
Beast Ransomware Group Targets Canadian Clinic Lessard Dental	https://malware.news/t/beast-ransomware-group-targets-canadian-clin...	T3
Ransomware Group beast Hits: Lessard Dental - HookPhish	https://www.hookphish.com/blog/ransomware-group-beast-hits-lessard-...	T3
Ransomware Alert: Lessard Dental, a Canada-based Hospital ...	https://x.com/FalconFeedsio/status/2047615493524320576	T3
Ransomware group Beast has targeted Lessard Dental, a family ...	https://x.com/TweetThreatNews/status/2047642992622674150	T3

Generated 2026-04-26 13:29 UTC by TJS Security Command Center