INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-28 06:46 UTC

# Silent Ransom Group Targets Law Firms with In-Person Social Engineering, FBI Warns

THREAT ACTOR | HIGH | CVSS 7.5

| | |
|---|---|
| SCC Item ID | SCC-TAC-2026-0020 |
| Type | Threat Actor |
| Severity | HIGH |
| CVSS Base Score | 7.5 |
| Affected Products | Law firm servers and databases (sector-wide; no specific vendor products identified) |
| Published | 2026-05-27T16:38:01 |
| Discovery Source | Rss |

## Executive Summary

The FBI has issued an advisory warning that Silent Ransom Group (SRG) is targeting law firms using a hybrid attack model that combines in-person social engineering with remote intrusion to gain unauthorized access to servers and databases holding privileged legal data. Once inside, SRG exfiltrates client records, litigation strategy, and sensitive financial information, then uses that data as extortion leverage. Law firms face significant exposure because attorney-client privilege protections and professional confidentiality obligations create disincentives to disclose breaches publicly, a dynamic SRG may exploit to increase negotiating pressure.

## Technical Analysis

Silent Ransom Group (SRG) is conducting financially motivated extortion campaigns against the legal sector. The group's current methodology combines physical presence at target facilities with social engineering and pretexting (T1598, T1566) to deceive employees and bypass logical access controls. Operatives impersonate vendors, IT personnel, or other trusted parties to gain physical access and obtain credentials. Once inside, SRG uses valid accounts (T1078), gathers victim organization information (T1591), and accesses data repositories (T1213). No CVEs are associated with this campaign; the primary attack surface is human-layer and physical access controls. Relevant CWEs include CWE-284 (Improper Access Control), CWE-306 (Missing Authentication for Critical Function), and CWE-522 (Insufficiently Protected Credentials). Post-access, SRG exfiltrates data and applies extortion pressure (T1657) without deploying ransomware encryption in recent campaigns, distinguishing this group from traditional ransomware-as-a-service operations. MITRE ATT&CK techniques in use: T1078 (Valid Accounts), T1591 (Gather Victim Org Information), T1598 (Phishing for Information), T1213 (Data from Information Repositories), T1566 (Phishing), T1657 (Financial Theft). No patch

exists; remediation is entirely procedural and control-based.

## Action Checklist

1. Containment, Immediately audit all active sessions and accounts on systems holding client data, case files, and financial records. Revoke any sessions or credentials that cannot be attributed to a verified, authorized user. Per NIST AC-2, review account types and disable any accounts that cannot be confirmed as authorized. Enforce badge and visitor log reviews for any unrecognized physical access in the past 30 days.
2. Detection, Review physical access logs (badge readers, visitor sign-in) for unrecognized individuals or tailgating incidents over the past 60 days. Correlate with authentication logs (NIST AU-2, AU-6) for logins occurring outside normal business hours or from unfamiliar workstations. Alert on new accounts, privilege escalations, and large data transfers to external destinations. Use Local Account Monitoring (D3-LAM) to flag dormant or newly created local accounts. Query endpoint and server logs for bulk file access or staging activity consistent with data exfiltration.
3. Eradication, Enforce MFA on all systems containing client or case data (NIST AC-17, CIS 6.3, 6.4, 6.5; D3-MFA). Rotate credentials for any account that had access to sensitive repositories (D3-CRO). Implement or tighten visitor management procedures, requiring verified identification and escorted access for all non-employees. Disable any accounts not required for current business operations (CIS 5.3). Review and harden remote access configurations per NIST AC-17.
4. Recovery, Verify that all active accounts align with the authorized account inventory (NIST AC-2, CIS 5.1). Confirm MFA is enforced and logging is active across all sensitive systems (NIST AU-12, CIS 8.2). Monitor for re-entry attempts using known SRG behavioral patterns: repeated contact from unfamiliar individuals, unsolicited IT support visits, and anomalous data access volumes. Validate that audit storage capacity is sufficient for extended retention (NIST AU-4, AU-11).
5. Post-Incident, Conduct a control gap review against NIST AC-3 (Access Enforcement), AC-6 (Least Privilege), and AC-5 (Separation of Duties). Evaluate physical security posture: visitor policies, reception protocols, and employee security awareness training specific to in-person social engineering. Map identified gaps to CIS 4.6 (Securely Manage Enterprise Assets) and CIS 6.1 (Access Granting Process). Document lessons learned and update the incident response playbook to include physical access scenarios.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |
| **Escalation Criteria** | Escalate immediately to firm leadership, outside breach counsel, and the FBI (IC3.gov) if any confirmed unauthorized access to client matter files, litigation strategies, or financial records is identified, or if SRG extortion contact is received, as this triggers potential breach notification obligations under applicable state bar ethics rules (ABA Model Rule 1.6) and state data breach notification statutes. |

| | |
|---|---|
| **Recovery Notes** | Post-containment, maintain elevated monitoring of DMS access logs, VPN authentication logs, and physical visitor records for a minimum of 90 days, as SRG may have established secondary persistence mechanisms (installed remote access tools, backdoor accounts) during any physical access period that survived initial eradication. Verify integrity of client data repositories by comparing current file hashes or DMS version histories against pre-incident backups to establish whether exfiltration occurred and what data is at risk for extortion leverage. Do not restore from backup without first confirming the backup predates the earliest suspected SRG access date established by the physical-digital correlation timeline. |
| **Forensic Artifacts** | Document Management System (DMS) audit logs (iManage Work, NetDocuments, or equivalent) — SRG targets litigation strategy and client financial records specifically; export access logs for all matter files filtered by accounts accessing practice groups outside their normal assignment or accessing high volumes of documents in a single session, which is the digital signature of SRG's bulk exfiltration staging behavior. \| Windows Security Event Log Event IDs 4624/4648/4720/4732/4670 on file servers and domain controllers — these events document the account creation, privilege escalation, and lateral movement sequence that SRG uses after gaining initial access, whether through a compromised credential obtained via in-person social engineering or a remotely installed tool. \| Badge reader controller audit export and visitor sign-in logs covering 60 days prior to incident — SRG's defining characteristic is combining physical reconnaissance or access with remote intrusion; the visitor log is a primary forensic artifact for establishing the initial access timeline and identifying the specific operative(s) involved. \| Registry key 'HKLM\SYSTEM\CurrentControlSet\Services' and Windows Event ID 7045 (New Service Installed) on all servers — SRG operatives posing as IT support during physical visits may install legitimate remote management tools (AnyDesk, TeamViewer, ScreenConnect) as persistence mechanisms that appear benign but enable ongoing remote access after the physical visit concludes. \| Network flow logs or Wireshark captures on the perimeter uplink filtered for large outbound transfers (sustained sessions over 10MB to non-corporate cloud destinations) during off-hours — SRG exfiltrates client records and financial data as extortion leverage, and bulk transfer events to personal cloud storage (Mega.nz, generic HTTPS endpoints) during evenings or weekends are the network-layer artifact of that exfiltration activity. |

### Per-Action IR Details

**Containment — Immediately audit all active sessions and accounts on systems holding client data, case files, and financial records. Revoke any sessions or credentials that cannot be attributed to a verified, authorized user. Per NIST AC-2, review account types and disable any accounts that cannot be confirmed as authorized. Enforce badge and visitor log reviews for any unrecognized physical access in the past 30 days.**

**NIST Phase:** Containment

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

**Controls:** NIST AC-2 (Account Management), NIST AC-12 (Session Termination), NIST IR-4 (Incident Handling), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

**Compensating:** Run 'query session /server:' on Windows to enumerate all active RDP and console sessions. Export with 'net user /domain > accounts_snapshot.txt' and diff against last known-good HR roster. For physical access, manually pull raw CSV exports from the badge reader controller (most systems support this without enterprise software) and sort by employee ID against active directory — flag any badge swipes from separated employees or visitor badges issued without a corresponding visitor log entry.

**Evidence:** BEFORE revoking sessions, capture full session state: run 'netstat -ano' and 'qwinsta /server:' on all affected servers to document active connections and session owners. Export Windows Security Event Log filtering on Event ID 4624 (Successful Logon) and 4648 (Explicit Credential Logon) for the past 30 days, focusing on Logon Type 3 (Network) and Type 10 (RemoteInteractive) from unfamiliar source IPs or workstations. Photograph or export visitor

log binders and badge controller audit trails before they are overwritten — SRG's physical reconnaissance phase may show as visitor entries with vague or inconsistent stated purposes (e.g., 'vendor support,' 'IT maintenance') cross-referencing no actual work order.

**Detection — Review physical access logs (badge readers, visitor sign-in) for unrecognized individuals or tailgating incidents over the past 60 days. Cross-reference with authentication logs (NIST AU-2, AU-6) for logins occurring outside normal business hours or from unfamiliar workstations. Alert on new accounts, privilege escalations, and large data transfers to external destinations. Use D3-LAM (Local Account Monitoring) to flag dormant or newly created local accounts. Query endpoint and server logs for bulk file access or staging activity consistent with data exfiltration.**

**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-3 (Content of Audit Records), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without a SIEM, use PowerShell on each file server holding client matter files: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4663}' to surface Object Access events on directories containing case files — sort by account name and timestamp to identify bulk reads inconsistent with normal attorney access patterns. Deploy Sysmon (config schema v4.82+) with EventID 11 (FileCreate) and EventID 23 (FileDelete) targeting document staging paths (e.g., C:\Users*\AppData\Local\Temp, any external share mount points). For network exfiltration, run Wireshark captures on the uplink interface filtering 'tcp.port==443 and frame.len > 1400' during off-hours to catch sustained large uploads characteristic of SRG bulk data staging.

**Evidence:** SRG's hybrid model means detection artifacts span two vectors: physical and digital. Capture visitor sign-in sheets and badge reader exports covering 60 days before any suspected intrusion date — SRG operatives conducting in-person reconnaissance may appear as repeat visitors or individuals who badged into areas beyond their stated access purpose. For the digital vector, pull Windows Security Event Log Event ID 4720 (Account Created) and 4732 (Member Added to Security-Enabled Local Group) to identify any accounts created after an unrecognized physical visit. Query DMS (Document Management System) access logs — iManage, NetDocuments, or equivalent — for accounts accessing matter files outside their assigned practice group, which is a strong SRG-specific indicator given their targeting of litigation strategy and client financial records.

**Eradication — Enforce MFA on all systems containing client or case data (NIST AC-17, CIS 6.3, CIS 6.4, CIS 6.5; D3-MFA). Rotate credentials for any account that had access to sensitive repositories (D3-CRO). Implement or tighten visitor management procedures, requiring verified identification and escorted access for all non-employees. Disable any accounts not required for current business operations (CIS 5.3). Review and harden remote access configurations per NIST AC-17.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication and Recovery

**Controls:** NIST AC-17 (Remote Access), NIST IA-5 (Authenticator Management), 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)

**Compensating:** For MFA enforcement without an enterprise IdP, enable Windows Hello for Business or configure RADIUS-based MFA via Duo Security's free tier (up to 10 users) on VPN and RDP gateways. For credential rotation at scale with a 2-person team, use the PowerShell snippet 'Get-ADUser -Filter * -Properties PasswordLastSet | Where-Object {$_.Enabled -eq $true} | ForEach-Object { Set-ADAccountPassword $_ -Reset -NewPassword (ConvertTo-SecureString -AsPlainText "TempPass$(Get-Random)!" -Force) }' to force resets, then require change at next logon. For visitor management hardening, implement a paper-based pre-authorization form requiring a named internal sponsor, government-issued ID scan, and escort assignment — this is specifically designed to defeat SRG's tactic of presenting as IT vendors or support personnel without pre-scheduled work orders.

**Evidence:** Before rotating credentials, preserve a full snapshot of account privilege assignments: export 'Get-ADGroupMember -Identity "Domain Admins" -Recursive' and all security group memberships for accounts with access to the DMS and financial systems. This documents the blast radius of any SRG-compromised credential and is

required for breach notification analysis. Capture Windows Security Event Log Event ID 4670 (Permissions on an Object Changed) and Event ID 4728/4732/4756 (Group Membership Changes) for the 60-day lookback window — SRG may have quietly elevated a compromised account to facilitate persistent access before triggering extortion, and these events are your forensic record of that escalation path.

**Recovery — Verify that all active accounts align with the authorized account inventory (NIST AC-2, CIS 5.1). Confirm MFA is enforced and logging is active across all sensitive systems (NIST AU-12, CIS 8.2). Monitor for re-entry attempts using known SRG behavioral patterns: repeated contact from unfamiliar individuals, unsolicited IT support visits, and anomalous data access volumes. Validate that audit storage capacity is sufficient for extended retention (NIST AU-4, AU-11).**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST AC-2 (Account Management), NIST AU-4 (Audit Storage Capacity), NIST AU-11 (Audit Record Retention), NIST AU-12 (Audit Record Generation), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 8.2 (Collect Audit Logs)

**Compensating:** Use osquery with the query 'SELECT uid, username, description, shell FROM users WHERE shell != "/sbin/nologin";' scheduled hourly on all servers to continuously reconcile active accounts against a baseline CSV of authorized staff — pipe output differences to a local alert log reviewed each morning. For log storage capacity, calculate retention needs as: (daily log volume in MB) x 90 days, then provision accordingly using Windows built-in log archiving ('wevtutil al Security.evtx /l:C:\LogArchive\') on a dedicated drive or NAS volume. For re-entry monitoring specific to SRG's in-person vector, brief reception staff to log all unsolicited IT-related visitor contacts and route them to a designated security email alias for same-day review.

**Evidence:** During recovery monitoring, maintain a running comparison of DMS access logs against the pre-incident baseline to detect any residual unauthorized access that survived eradication — SRG may have implanted a secondary credential or maintained a persistent remote access mechanism (e.g., a legitimately installed remote management tool like AnyDesk or TeamViewer installed under the guise of IT support during a physical visit). Check Windows Event ID 7045 (New Service Installed) and the registry key 'HKLM\SYSTEM\CurrentControlSet\Services' for any remote access tools installed within the 60-day lookback window that do not align with your authorized software inventory per CIS 2.1.

**Post-Incident — Conduct a control gap review against NIST AC-3 (Access Enforcement), AC-6 (Least Privilege), and AC-5 (Separation of Duties). Evaluate physical security posture: visitor policies, reception protocols, and employee security awareness training specific to in-person social engineering. Map identified gaps to CIS 4.6 (Securely Manage Enterprise Assets) and CIS 6.1 (Access Granting Process). Document lessons learned and update the incident response playbook to include physical access scenarios.**

**NIST Phase:** Post Incident

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

**Controls:** NIST AC-3 (Access Enforcement), NIST AC-5 (Separation of Duties), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST PM-16 (Threat Awareness Program), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 6.1 (Establish an Access Granting Process)

**Compensating:** For the control gap review without GRC tooling, build a spreadsheet mapping each AC-3, AC-5, and AC-6 control requirement to a named system owner and current implementation status — focus specifically on the DMS, billing system, and any shared drives holding client matter files, as these are SRG's primary targets. For security awareness training specific to SRG's in-person tactics, conduct a 30-minute tabletop exercise with reception and paralegal staff using a realistic scenario: 'An individual arrives claiming to be from your IT managed service provider to perform an emergency server update; what do you do?' Document the playbook update to include a physical intrusion decision tree: (1) verify caller/visitor identity against a pre-approved vendor list, (2) contact the named internal sponsor directly before granting access, (3) escalate to firm management if identity cannot be confirmed.

**Evidence:** The post-incident review must produce a documented timeline correlating physical access events (visitor logs, badge swipes) with digital authentication events (Event ID 4624, 4648) and data access events (DMS audit logs, Event ID 4663) — this correlation is the definitive forensic artifact establishing SRG's attack chain for this incident and

is required for any regulatory breach notification analysis under applicable state bar rules or ABA Model Rule 1.6 cybersecurity obligations. Preserve all raw log exports, badge controller data, visitor sign-in records, and account change logs in an evidence archive with SHA-256 hashes documented at time of collection, maintaining chain of custody in the event of law enforcement referral per FBI advisory guidance.

## Detection Guidance

Detection for SRG activity requires correlating physical and logical access signals. Monitor authentication logs for valid credential use outside expected hours, from unfamiliar internal workstations, or following a reported visitor interaction. Per NIST AU-6, review audit records regularly for anomalous access to document management systems, case databases, and file shares. Apply Local Account Monitoring (D3-LAM) to detect newly created or reactivated local accounts. Flag bulk file reads, archive creation (ZIP, RAR), and data transfers to cloud storage or external IP addresses. Review physical access records (badge swipes, visitor logs) for unrecognized entries or gaps. SRG operatives use social pretexting; correlate any reports of suspicious visitors or unsolicited IT support requests with subsequent system access events. SIEM correlation rule: valid account login + off-hours access + large outbound data transfer within the same session.

## Framework Mappings

### MITRE-ATTACK

- **T1078** — Valid Accounts
- **T1591** — Gather Victim Org Information
- **T1200** — Hardware Additions
- **T1213** — Data from Information Repositories
- **T1598** — Phishing for Information
- **T1486** — Data Encrypted for Impact
- **T1657** — Financial Theft
- **T1566** — Phishing

### NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **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
- **AC-3** — Access Enforcement

### OWASP-TOP10-2021

- **A01:2021** — Broken Access Control
- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design

### CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **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
- **CC6.3** — Authorizes, modifies, or removes access

### HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(6)(ii)** — Response and Reporting

### ISO-27001-2022

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

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1078 | Valid Accounts | Defense-Evasion |
| T1591 | Gather Victim Org Information | Reconnaissance |
| T1200 | Hardware Additions | Initial-Access |
| T1213 | Data from Information Repositories | Collection |
| T1598 | Phishing for Information | Reconnaissance |
| T1486 | Data Encrypted for Impact | Impact |
| T1657 | Financial Theft | Impact |
| T1566 | Phishing | Initial-Access |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.darkreading.com/cyberattacks-data-breaches/ransomware-a... | T3 |
| **Software vendor refuses to fix security vulnerability - what to do?** | https://security.stackexchange.com/questions/264626/software-vendor... | T3 |
| **Lawyers Encouraged to Vet Tech Vendors Carefully** | https://www.esquiresolutions.com/lawyers-encouraged-to-vet-tech-ven... | T3 |
| **Security Vendor - an overview \| ScienceDirect Topics** | https://www.sciencedirect.com/topics/computer-science/security-vendor | T3 |
| **[PDF] Ensuring Vendors Aren't The Weak Link In Your Security Chain** | https://www.porterwright.com/content/uploads/2019/02/Ensuring-Vendo... | T3 |



Generated 2026-05-28 06:46 UTC by TJS Security Command Center