INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-27 14:07 UTC

Silent Ransom Group (Luna Moth) Conducts Physical Impersonation Attacks Against Law Firms

THREAT CAMPAIGN | **HIGH** | CVSS 7.8

SCC Item ID	SCC-CAM-2026-0372
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.8
Affected Products	Law firms (primary); insurance, finance, and healthcare sectors (secondary/potential)
Published	2026-05-27
Discovery Source	Gemini

Executive Summary

The FBI has warned that Silent Ransom Group (SRG), also tracked as Luna Moth, is now sending operatives in person to law firm offices, posing as IT staff to gain direct physical access to workstations and internal systems. This physical impersonation tactic extends their established callback phishing operation and bypasses technical security controls entirely. Law firms face direct exposure of privileged client data through extortion threats; insurance, finance, and healthcare organizations with comparable data sensitivity are assessed as secondary targets.

Technical Analysis

Silent Ransom Group operates a data-extortion model without ransomware encryption. Their established tradecraft uses callback phishing (MITRE T1566.004, T1566), targets receive emails directing them to call a phone number where SRG actors manipulate victims into installing remote access tools (T1219) or surrendering credentials (T1078, T1598). The physical impersonation vector (T1204) layers on top: operatives present in person as IT personnel to gain unsupervised workstation access, enabling direct data collection (T1213, T1530) and extortion (T1657). No CVE is associated; the attack chain exploits procedural and human control failures mapped to CWE-522 (insufficiently protected credentials), CWE-284 (improper access control), CWE-306 (missing authentication for critical function), and CWE-1390 (weak authentication). No ransomware payload is deployed; exfiltrated legal data is threatened for public release. Physical access attempts represent an escalation specifically designed to circumvent network-layer and endpoint controls.

Action Checklist

1. Step 1: Containment. Immediately implement a mandatory IT staff identity verification protocol. Any in-person IT access request must be validated against a pre-approved vendor/staff roster with photo ID cross-checked by a manager or reception supervisor before workstation access is permitted. Notify all office managers and front-desk staff today (NIST IR-6: Incident Response, Post-Incident Activities; CIS 6.1: Secure User Access Management).
2. Step 2: Detection. Review physical access logs, visitor logs, and badge entry records for unscheduled or unverified IT visits in the past 90 days. Correlate against remote access tool (RAT) installation events in endpoint logs, look for AnyDesk, Zoho Assist, or similar tool installations initiated outside IT change management windows. Review AU-2 and AU-12 log sources for account access anomalies coinciding with any unscheduled physical visits.
3. Step 3: Eradication. Audit all workstations accessed by unverified personnel; remove any unauthorized remote access tools. Reset credentials for any accounts accessed during suspect sessions (NIST AC-2: Account Management; D3-CRO: Credential Rotation Observability). Revoke and reissue any API keys or privileged credentials on systems that were physically accessed without documented authorization.
4. Step 4: Recovery. Validate endpoint integrity on affected workstations using system file analysis (D3-SFA: System File Analysis). Re-enable MFA on all accounts that touched affected systems (NIST IA-2: Authentication; CIS 6.3, 6.5: Multi-Factor Authentication). Monitor for outbound data transfers to unknown destinations for a minimum of 30 days post-incident, given SRG's data exfiltration focus (NIST SI-4: Information System Monitoring; AU-6: Audit Review, Analysis, and Reporting).
5. Step 5: Post-Incident. Conduct a tabletop exercise simulating a physical impersonation attempt. Document and close the control gap between physical security and IT access procedures. Implement a formal visitor management policy requiring pre-authorization for all IT vendor access (NIST PE-3: Physical Access Control; AC-3: Access Enforcement; CIS 4.6: Secure Configuration Management). Brief staff on callback phishing and physical social engineering as paired tactics, this is a combined human-layer attack, and staff awareness is the primary control.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to outside legal counsel, law enforcement (FBI IC3), and trigger breach notification assessment if any confirmed unauthorized physical access to workstations is identified, any evidence of DMS data exfiltration is found, or if affected systems contain PHI, PII, or privileged client communications subject to state breach notification statutes or HIPAA.
Recovery Notes	Post-containment, maintain enhanced outbound network monitoring for a minimum of 30 days given SRG's documented pattern of staging exfiltrated data over extended periods before issuing extortion demands. Revalidate MFA enrollment on all accounts weekly for the first month to detect any credential persistence SRG may have established during physical access. Law firms should engage their cyber insurance carrier immediately, as SRG specifically targets firms with cyber liability coverage and tailors extortion demands to policy limits.

Forensic Artifacts	AnyDesk trace logs at C:\Users*\AppData\Roaming\AnyDesk\ad.trace and ad_svc.trace — record the remote AnyDesk ID of the SRG operator, session timestamps, and source IP addresses used during the physical access window | Windows Prefetch files at C:\Windows\Prefetch\ANYDESK*.pf and ZOHOASSIST*.pf — establish first and last execution timestamps for any RAT installed by the operative, corroborating the physical visit timeline | Document Management System (NetDocuments, iManage) audit logs filtered for bulk document opens, downloads, or exports within the 72-hour window of each unscheduled visit — SRG's primary objective is privileged client data exfiltration from law firm DMS platforms | Windows Security Event ID 4648 (Logon Using Explicit Credentials) and Event ID 4663 (Object Access Attempt) timestamped to the visit window — identify which accounts were used and which file system objects were accessed by the operative during the session | Physical visitor logs, reception sign-in sheets, and badge/keycard access system exports for the 90-day lookback period — when correlated with RAT installation timestamps, these establish the physical-to-digital kill chain and identify the full scope of SRG operative visits across all office locations

Per-Action IR Details

Step 1: Containment — Immediately implement a mandatory IT staff identity verification protocol. Any in-person IT access request must be validated against a pre-approved vendor/staff roster with photo ID cross-checked by a manager or reception supervisor before workstation access is permitted. Notify all office managers and front-desk staff today (NIST IR-6, CIS 6.1).

NIST Phase: Containment

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

Controls: NIST IR-6 (Incident Reporting), NIST PE-3 (Physical Access Control), NIST PS-6 (Access Agreements), CIS 6.1 (Establish an Access Granting Process)

Compensating: Distribute a one-page laminated verification card to every reception desk and office manager today listing: (1) the names and photos of all authorized IT staff and vendors, (2) the IT helpdesk direct line to call-back-verify any unscheduled visit, and (3) a hard rule — no workstation access before verbal confirmation from IT management. Maintain a paper visitor log with time-in, time-out, purpose, and authorizing manager signature. Zero-cost and deployable in under two hours.

Evidence: Before issuing the protocol, photograph and preserve all existing physical visitor logs, badge entry printouts, and reception sign-in sheets covering the past 90 days. These are your pre-containment baseline. Document the date/time the protocol was communicated to each office location so you can establish a clear before/after boundary if a prior SRG operative visit is later identified.

Step 2: Detection — Review physical access logs, visitor logs, and badge entry records for unscheduled or unverified IT visits in the past 90 days. Correlate against remote access tool (RAT) installation events in endpoint logs — look for AnyDesk, Zoho Assist, or similar tool installations initiated outside IT change management windows. Review AU-2 and AU-12 log sources for account access anomalies coinciding with any unscheduled physical visits.

NIST Phase: Detection Analysis

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

Controls: NIST AU-2 (Event Logging), NIST AU-12 (Audit Record Generation), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

Compensating: Run the following PowerShell on each endpoint to surface AnyDesk, Zoho Assist, Splashtop, or ScreenConnect installs outside IT-managed software: `Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Where-Object {$_.DisplayName -match 'AnyDesk|Zoho|Splashtop|ScreenConnect'} | Select DisplayName, InstallDate, InstallSource`. Cross-reference install timestamps against your paper visitor log. For Sysmon-enabled endpoints, query Event ID 11 (FileCreate) and Event

ID 13 (RegistrySet) for AnyDesk's default install path `C:\Users\*\AppData\Roaming\AnyDesk\` and registry key `HKCU\Software\AnyDesk`. Where Sysmon is absent, deploy it immediately using SwiftOnSecurity's baseline config before proceeding.

Evidence: Preserve the following before any remediation: (1) Windows Event Log — Security Event ID 4688 (Process Creation) filtered for `AnyDesk.exe`, `ZohoAssist.exe`, `agent.exe` (Zoho), `strwinclt.exe` (Splashtop) spawned by user-context processes rather than IT management tools; (2) prefetch files at `C:\Windows\Prefetch\ANYDESK*.pf` showing first and last execution timestamps; (3) AnyDesk trace logs at `C:\Users\*\AppData\Roaming\AnyDesk\ad.trace` and `ad_svc.trace` which record incoming connection IDs and IP addresses used by the SRG operative; (4) Windows Security Event ID 4624 (Successful Logon) and 4648 (Explicit Credential Use) timestamped within the unscheduled visit window; (5) browser history and download folder contents on visited workstations for any tooling dropped via web-based delivery during the physical access window.

Step 3: Eradication — Audit all workstations accessed by unverified personnel; remove any unauthorized remote access tools. Reset credentials for any accounts accessed during suspect sessions (NIST AC-2, D3-CRO — Credential Rotation). Revoke and reissue any API keys or privileged credentials on systems that were physically accessed without documented authorization.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-2 (Account Management), NIST AC-6 (Least Privilege), NIST CM-7 (Least Functionality), NIST IA-5 (Authenticator Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Use `sc query` and `Get-Service` to enumerate running services; cross-reference against a known-good baseline. Uninstall AnyDesk silently with `msiexec /x {AnyDesk-GUID} /quiet` or the AnyDesk CLI `--remove`. Kill persistence via: `reg delete HKCU\Software\Microsoft\Windows\CurrentVersion\Run /v AnyDesk /f`. For credential rotation without an enterprise PAM tool, use Active Directory Users and Computers to force password reset at next logon for all accounts with logon events during the suspect window, and immediately disable any service accounts that were accessed. Revoke document management system tokens (e.g., NetDocuments, iManage) via their admin consoles — SRG specifically targets law firm DMS platforms for privileged client data.

Evidence: Before removing any tool, capture a forensic image or at minimum a memory dump of the affected workstation using WinPmem (`winpmem_mini_x64.exe output.raw`) to preserve in-memory artifacts of the RAT session — AnyDesk keeps session keys in process memory. Also preserve: (1) AnyDesk `ad.trace` log showing the remote ID of the SRG operator; (2) Windows Security Event ID 4663 (Object Access) on DMS folders accessed during the session; (3) `$MFT` and `$LogFile` from the NTFS volume to reconstruct file access and staging activity; (4) Registry hive `NTUSER.DAT` for the logged-on user account to identify any persistence mechanisms or new scheduled tasks added by the operative.

Step 4: Recovery — Validate endpoint integrity on affected workstations using system file analysis (D3-SFA). Re-enable MFA on all accounts that touched affected systems (NIST IA-2, CIS 6.3, 6.5, D3-MFA). Monitor for outbound data transfers to unknown destinations for a minimum of 30 days post-incident, given SRG's data exfiltration focus (NIST SI-4, AU-6).

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IA-2 (Identification and Authentication — Organizational Users), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CP-10 (System Recovery and Reconstitution), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Run `sfc /scannow` on affected workstations as a baseline system file check. For DMS integrity, compare current document access/modification timestamps in NetDocuments or iManage audit logs against the pre-visit baseline — SRG's goal is bulk exfiltration, so look for large volumes of document opens or downloads in short time windows. For outbound transfer monitoring without a SIEM, deploy Zeek (formerly Bro) or enable Windows Firewall logging (`netsh advfirewall set allprofiles logging filename`) and parse with a daily cron/scheduled task piping output to a grep filter for known SRG exfil infrastructure or anomalous large-payload POST requests. Monitor

specifically for outbound connections to Mega.nz, PrivatBin, or newly-registered domains — SRG's documented exfiltration infrastructure.

Evidence: Before restoring workstations to production, collect and preserve: (1) Zeek or Windows Firewall connection logs showing any outbound data volumes exceeding baseline during and after the visit window; (2) DMS audit trail exports (NetDocuments Activity Report, iManage Work audit log) for the 72-hour window around each suspect visit, filtered for bulk download or export events; (3) browser history and `%TEMP%` directory contents for any staging archives (`.zip`, `.7z`, `.rar`) created during the session; (4) VSS (Volume Shadow Copy) snapshots if available — `vssadmin list shadows` — to enable before/after file system comparison. Do not delete shadow copies until forensic review is complete.

Step 5: Post-Incident — Conduct a tabletop exercise simulating a physical impersonation attempt. Document and close the control gap between physical security and IT access procedures. Implement a formal visitor management policy requiring pre-authorization for all IT vendor access (NIST PE-3, AC-3, CIS 4.6). Brief staff on callback phishing and physical social engineering as paired tactics — this is a combined human-layer attack, and staff awareness is the primary control.

NIST Phase: Post Incident

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

Controls: NIST PE-3 (Physical Access Control), NIST AC-3 (Access Enforcement), NIST AT-2 (Literacy Training and Awareness), NIST AT-3 (Role-Based Training), NIST IR-4 (Incident Handling), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: Tabletop scenario script (no-cost): Have a volunteer walk into reception claiming to be from 'IT support' referencing a recent phishing email complaint (mirroring SRG's callback lure) and request workstation access. Score staff response against the verification checklist from Step 1. For ongoing awareness, distribute CISA's Physical Security Awareness fact sheet and brief staff specifically on SRG's dual-vector pattern: the scam begins with a callback phishing email or voicemail, and the in-person visit is the second stage — staff who received any unusual IT-related voicemails or emails in the weeks before an unscheduled visit should be treated as potential SRG targets and interviewed. Document lessons learned in a formal after-action report referencing the specific control gaps this campaign exploited: no physical-to-IT access correlation, no RAT installation alerting, no DMS bulk-download detection.

Evidence: For post-incident documentation, preserve: (1) the complete timeline correlating physical visit records with endpoint RAT installation events and DMS access anomalies — this is your incident reconstruction artifact; (2) staff interview notes from any employees who interacted with the SRG operative, capturing the social engineering pretext used (IT helpdesk uniform, badge appearance, stated purpose); (3) any voicemails or emails that preceded the physical visit, which constitute the callback phishing artifact and establish the full SRG kill chain for the record; (4) before/after screenshots of visitor log and badge access policy documentation to evidence the control improvement for any regulatory or client notification obligations.

Detection Guidance

There are no network-based IOCs published for this campaign at this time. Detection relies on behavioral and procedural indicators. Physical layer: audit visitor logs and badge access records for unscheduled entries by individuals claiming IT affiliation. Endpoint layer: query for installation events of known remote access tools (AnyDesk, Zoho Assist, Splashtop, TeamViewer, ConnectWise) outside approved change windows, correlate install timestamps against visitor log entries. Identity layer: look for credential use from unfamiliar source IPs or devices immediately following a reported or logged physical visit. Email layer: hunt for callback phishing lures, emails with no malicious attachment or link but containing a phone number and urgency language (billing, subscription cancellation, IT support). SIEM correlation rule: flag any RAT installation event on a workstation located in a physical office within 24 hours of an unscheduled visitor entry. Monitor for large outbound file transfers (T1530, T1213) from workstations that logged anomalous local access events. D3-LAM (Local Account

Monitoring) and D3-SFA (System File Analysis) are the relevant D3FEND countermeasures for endpoint-side detection.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs published`	The FBI advisory and available reporting do not include specific IP addresses, domains, or file hashes attributed to this campaign at this time. Organizations should monitor for behavioral indicators described in detection_guidance.	LOW

Framework Mappings

MITRE-ATTACK

- **T1219** — Remote Access Tools
- **T1566** — Phishing
- **T1078** — Valid Accounts
- **T1566.004** — Spearphishing Voice
- **T1598** — Phishing for Information
- **T1213** — Data from Information Repositories
- **T1657** — Financial Theft
- **T1530** — Data from Cloud Storage
- **T1204** — User Execution

NIST-800-53R5

- **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-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AC-3** — Access Enforcement
- **CP-9** — System Backup
- **IR-4** — Incident Handling

- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

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

CIS-V8

- **5.2** — Use Unique Passwords
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(a)(1)** — Access Control
- **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
- **164.312(e)(1)** — Transmission Security

SOC2-TSC

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

NIST-CSF-2

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

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
T1219	Remote Access Tools	Command-And-Control
T1566	Phishing	Initial-Access
T1078	Valid Accounts	Defense-Evasion
T1566.004	Spearphishing Voice	Initial-Access

Technique ID	Technique Name	Tactic
T1598	Phishing for Information	Reconnaissance
T1213	Data from Information Repositories	Collection
T1657	Financial Theft	Impact
T1530	Data from Cloud Storage	Collection
T1204	User Execution	Execution

Sources

Source	URL	Tier
gemini	https://www.helpnetsecurity.com/2026/05/27/silent-ransom-group-phys...	T3
Data Strategy, Security & Privacy | Practices - Holland & Knight	https://www.hklaw.com/en/services/practices/technology-and-cybersec...	T2
Law Firms Are Under Siege: Deepfakes, Data Breaches & Email ...	https://www.infoguardsecurity.com/law-firms-are-under-siege-deepfak...	T3
Cyber Insurance for Law Firms: What Attorneys Need to Know	https://www.legalfuel.com/cyber-insurance-for-law-firms-what-attorn...	T3
Legal implications for clinicians in cybersecurity incidents: A review	https://pmc.ncbi.nlm.nih.gov/articles/PMC11441973/	T1

Generated 2026-05-27 14:07 UTC by TJS Security Command Center