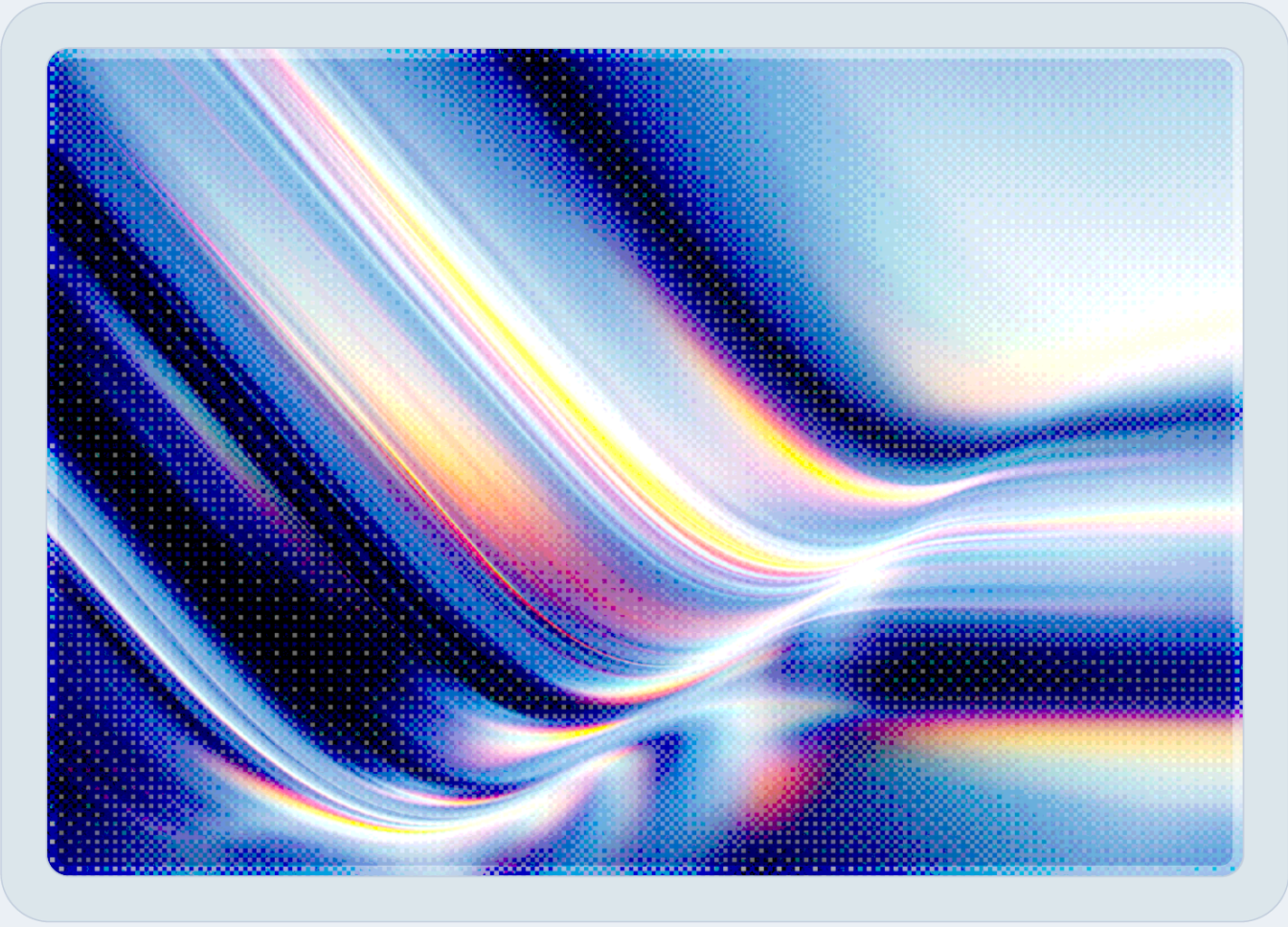
CSAI Foundation | Cloud Security Alliance

Silent Ransom Group: Vishing and Physical Intrusion at Law Firms

How UNC3753's Multi-Vector Campaign Threatens Legal and Financial Services

2026-06-08

AI-assisted Rapid Research



CSAI

CSA cloud security alliance®

Key Takeaways

- UNC3753 (also tracked as Silent Ransom Group, Luna Moth, and Chatty Spider) has conducted a sustained and expanding data theft extortion campaign against U.S. legal and financial services firms since at least January 2026, adding physical office intrusion as a new tactic; the FBI issued a FLASH advisory on May 26, 2026 [1].
- The group combines invoice-themed email priming, voice phishing (vishing), real-time screen-sharing hijack, commercial remote monitoring and management (RMM) tool abuse, and in some cases physical office intrusion — all within a single business day [2].
- Mandiant/Google Threat Intelligence Group observed the complete attack lifecycle — from first contact to data exfiltration and extortion demand — completing in under one hour in the most recent incidents [2].
- The group's data leak site, LEAKEDDATA (hosted at business-data-leaks[.]com), had published data from at least 38 law firms as of late May 2026, with the total victim count across all sectors exceeding 100 organizations [3].
- No traditional ransomware encryption is deployed; the threat is purely data theft paired with explicit threats of client notification, regulatory reporting, and data publication as extortion leverage [2].
- CSA recommends organizations treat the following as immediate defensive priorities: vishing awareness training for all staff, strict verification protocols for inbound IT requests, conditional access policies limiting VDI to corporate-managed devices, and physical access controls requiring escort and credential verification for any unscheduled technician visit.

Background

UNC3753 is a financially motivated threat cluster that has operated since at least March 2022 and is tracked by Google's Mandiant Threat Intelligence Group under the aliases Luna Moth and Chatty Spider, and by the FBI as Silent Ransom Group [1][2]. Mandiant has assessed that its earliest campaigns were closely related to UNC2686, the group responsible for the Bazarcall callback-phishing operations that used fraudulent subscription cancellation notices to lure targets into calling attacker-controlled phone

numbers — a technique that subsequently spread to multiple criminal affiliates [2]. In 2022, UNC3753 deployed the LOCKBIT.BLACK ransomware in at least some intrusions, but by 2025 the group had abandoned encryption entirely in favor of pure data exfiltration and extortion [2].

The tactical pivot that defines UNC3753's current campaign began in earnest in March 2025. Rather than relying on subscription-billing lures with embedded PDF attachments, the group shifted to impersonating its victims' own internal IT helpdesks — a change that Mandiant assesses likely increased success rates because it inverted the trust relationship [2]. Instead of asking a target to call an external number, attackers call the target directly from spoofed or actor-registered numbers, presenting themselves as familiar internal support personnel responding to a ticket or alert. This shift is significant because it exploits the trust employees instinctively extend to their own IT teams — a relationship in which employees are conditioned to accept direction and grant access with minimal independent verification.

Between January and May 2026, Mandiant investigated dozens of UNC3753 intrusions concentrated in U.S. professional, legal, and financial services organizations. The FBI corroborated these findings in a TLP:CLEAR FLASH advisory (FLASH-20260526-01) issued on May 26, 2026, noting that the group had added physical office intrusion as a fallback tactic when remote social engineering failed [1][4]. Specific named victims whose data was published on the LEAKEDDATA site include Orrick, Herrington & Sutcliffe, as well as Jones Day and Wood Smith Henning & Berman [5].

The targeting of legal services is not accidental. Law firms are custodians of concentrated, high-value repositories of sensitive data including client trade secrets, merger and acquisition plans, regulatory compliance files, and personal information for corporate executives and employees alike. Because law firms' core commercial value is their clients' trust and confidentiality, even the credible threat of public data exposure creates enormous pressure to pay — making legal services among the most economically rational targets for extortion-only campaigns.

Security Analysis

The Multi-Vector Attack Chain

UNC3753's intrusions begin with a low-risk priming step: benign, invoice-themed emails sent from actor-controlled consumer email accounts to targeted individuals. These emails contain no malicious links or attachments — they are designed solely to establish a false pretext, so that when an attacker calls

the recipient hours or days later claiming to follow up on "the invoice," the conversation does not begin cold [2]. The group targets personnel across all seniority levels, sourcing contact information from corporate websites, LinkedIn, and public legal directories.

The vishing call itself relies on impersonating the victim organization's own IT helpdesk or information security team. Attackers establish urgency — a claimed security alert, a pending data migration, a compliance audit — and instruct the target to open a screen-sharing session via Zoom, Microsoft Teams, Quick Assist, or Windows Terminal Services. Mandiant observed one intrusion in which the victim participated in five distinct Teams video calls over three days before the attacker achieved sufficient access to begin exfiltration [2]. Once screen-sharing is established, attackers observe the target's environment and direct them to download and execute a commercial RMM agent: AnyDesk, Bomgar, Zoho Assist, SuperOps, or Syncro have all been observed in this campaign [2]. In multiple observed intrusions, installation links and commands were delivered via Privnote — a service that generates self-destructing links — to prevent the instructions from persisting in browser history or chat logs.

BYOD Pivoting and Enterprise System Access

UNC3753 has refined a technique of using compromised BYOD endpoints as a pivot into corporate infrastructure. During the screen-sharing phase, if the target is on a personal device, attackers observe or capture credentials for corporate virtual desktop infrastructure (VDI) and then connect directly using Windows 365 or Citrix clients [2]. This allows the attacker to operate from within the corporate VDI environment with the victim's full entitlements, bypassing network perimeter controls that might otherwise flag an unusual source IP. The commercial RMM agent installed on the personal device provides a persistent channel back to attacker infrastructure, while the VDI session gives access to corporate file shares and document management systems.

Once inside the corporate environment, UNC3753 immediately begins targeted data discovery. The group has demonstrated specific familiarity with the iManage document management platform used extensively by law firms, executing keyword-based searches to locate tax records (W-2, W-9, and 1099 forms), Social Security numbers, audit files, client agreements, and M&A transaction documents [2]. Files are staged in predictable locations — the user's Downloads folder or Windows Roaming profile path — before exfiltration. Mandiant documented one engagement where 1.7 GB was exfiltrated to a Google Drive account (subsequently disabled by Google) followed by 14.4 GB via WinSCP to attacker-controlled infrastructure [2]. In other cases, attackers have directed victims to send files from their own iManage repositories to actor-controlled consumer email addresses, adding a layer of legitimacy that can defeat data loss prevention controls tuned for outbound exfiltration rather than user-directed sends.

Physical Intrusion as Fallback

The FBI's May 2026 FLASH advisory documents a qualitatively new capability: when remote social engineering fails to achieve access, the group dispatches individuals to victim office locations in person [1][4]. These operatives present themselves as IT technicians responding to a service ticket or security incident. They tell receptionists or employees that they need to "image the device" or "create local backups" for a security remediation, then attempt to insert USB storage media into an endpoint and directly exfiltrate corporate data. Mandiant assesses with moderate confidence that these physical incidents are linked to UNC3753 based on structural overlaps in targeting patterns and timeline alignment, though limited forensic evidence from in-person incidents prevents definitive attribution [2].

This physical vector is particularly concerning for several reasons. Many organizations' security awareness programs, visitor management systems, and access controls are designed primarily around physical threats such as tailgating or unauthorized building entry — and may not adequately address a socially sophisticated operative who arrives with a plausible pretext, a confident demeanor, and accurate knowledge of the target firm's IT terminology and internal support processes. The operative's knowledge of the target is a product of the same open-source intelligence collection that drives the remote vishing phase, meaning organizations that have not responded to an initial remote attempt may face a follow-on physical attempt within days.

Extortion Mechanics and Escalation

Within approximately 30 minutes of completing data exfiltration, UNC3753 sends an initial extortion email from actor-controlled accounts [2]. The demand is calculated in its coercive structure, threatening to notify the victim organization's clients and employees directly, publish stolen archives on the LEAKEDDATA site, and characterize the incident to regulators in a manner designed to maximize compliance and litigation exposure. Victims are given a three-day window to initiate contact, after which the group carries out its notification and publication threats. Mandiant has confirmed that the group does follow through on these threats: the LEAKEDDATA data leak site had published data from at least 38 law firms and over 100 total organizations as of late May 2026 [3][5].

The absence of ransomware encryption is almost certainly a strategic choice rather than a capability limitation — the group deployed LOCKBIT.BLACK ransomware as recently as 2022 [2]. Encryption would alert security monitoring tools and trigger incident response protocols. A data theft and extortion operation that uses only legitimate tools — commercial RMM agents, WinSCP, Rclone, built-in screen-sharing platforms — generates substantially fewer detectable artifacts and can be completed before any automated detection fires. The group's infrastructure uses actor-registered domains following the

naming pattern `<organization>-itdesk[.]com`, `<organization>-it[.]com`, and `<organization>-helpdesk[.]com` to make callback caller IDs and email domains appear internal [2][6].

Threat Actor Evolution and Scale

The scale of confirmed victims understates the campaign's full reach. Many organizations that pay extortion demands do not publicly disclose the incident, and firms that do not maintain the forensic capability to identify the initial access vector may never link a data exposure to this group. The FBI observed a surge in attacks specifically targeting legal services [1], and Halcyon tracked 134 ransomware and data extortion incidents against law firms and legal services organizations in the first quarter of 2026 alone, with legal services representing more than 6% of all such incidents tracked in the period [3]. The Resecurity threat intelligence team has separately documented DNS fast-flux infrastructure used by Silent Ransom Group to resist takedown efforts, adding operational resilience to the group's attack platform [6].

The MITRE ATT&CK framework techniques most central to this campaign are T1566.004 (Phishing: Spearphishing Voice), T1219 (Remote Access Software), T1052.001 (Exfiltration Over Physical Medium), and T1567.002 (Exfiltration Over Web Service: Exfiltration to Cloud Storage). Defenders building detection use cases should give priority to these techniques and to anomalous use of commercial RMM agents in environments where their installation is not centrally managed.

Recommendations

Immediate Actions

Organizations in legal services and financial services should treat the UNC3753 campaign as an active threat requiring immediate defensive posture review, not a future risk to plan against. The first priority is user awareness: every person who handles inbound calls or support requests — including legal assistants, paralegals, operations staff, and executive assistants — should be briefed on the specific vishing pretext this group uses. Employees must know that any inbound call requesting screen access, RMM installation, or file transfer should be independently verified by calling the IT helpdesk back on a number retrieved from the internal directory, never from a number provided by the caller. This single verification step significantly disrupts the attack chain at an early and critical point.

Physical security protocols require immediate attention at all office locations. Reception and facilities staff must be trained to treat any unscheduled technician visit as requiring verification: confirmation of an open support ticket from the firm's own IT team, government-issued photo identification, and escort to and from the workstation. USB ports on workstations in public-facing areas and at reception should be disabled at the hardware or endpoint configuration level where possible. Any technician claiming a need for removable media should be required to have the firm's own IT staff physically present for the duration of the interaction.

Short-Term Mitigations

Conditional access policies should be reviewed and tightened to ensure that corporate VDI and VPN access is restricted to corporate-managed, compliant devices. The BYOD pivot technique documented by Mandiant depends entirely on attackers being able to use credentials obtained during a screen-sharing session to log into VDI from a personal device. Requiring device compliance certificates or hardware-bound MFA tokens as conditions for VDI access would significantly reduce the viability of this pivot path.

Network security teams should audit for and block unauthorized RMM agent installation and execution. Where commercial RMM tools are legitimately used for IT support, their usage should be centrally logged and any installation on an endpoint not managed by the IT team should trigger an alert. Network egress controls should flag and alert on WinSCP and Rclone traffic (particularly on port 22), bulk uploads to consumer file-sharing services such as Google Drive or Dropbox, and connections to self-destructing messaging services such as Privnote. iManage administrators should enable bulk-download and keyword-search alerting and require MFA step-up authentication before allowing large-volume document exports.

Security operations centers should add detections for domain names matching the `<organization>-itdesk[.]com` and `<organization>-it[.]com` naming conventions in DNS query logs and email headers, as well as the specific IOC IP addresses published in Google's Mandiant threat intelligence report [2]. Enrollment in threat intelligence feeds that track the LEAKEDDATA site will provide early warning if an organization's data appears in a staging or publication state before a public announcement.

Strategic Considerations

Law firms and financial services organizations should assess whether their current incident response plans adequately address the no-malware, pure data theft extortion scenario UNC3753 employs. Traditional IR playbooks are often structured around the ransomware encryption event as the triggering

indicator; in this campaign, by the time any automated alert fires, the exfiltration may already be complete. Tabletop exercises should include a scenario where the first notification of a security incident is an extortion email received 30 minutes after a routine-seeming IT support call, with no malware detected and no encrypted files.

Data governance programs should evaluate whether the concentration of sensitive client documents in document management systems such as iManage is appropriately protected by access controls, activity logging, and anomaly detection. The specificity of UNC3753's iManage keyword searches — targeting W-2 files, SSNs, and M&A documents — suggests the group conducts reconnaissance on the document management platforms used by target industries before launching campaigns. Organizations should assume that a sophisticated actor knows what their document management platform can search for and plan data protection accordingly.

Finally, legal and financial services firms should evaluate their public disclosure obligations in the event of a successful extortion. The combination of PII theft (W-2 forms, SSNs), client privileged information, and regulatory documents creates potential notification obligations under state breach notification laws, SEC disclosure rules for regulated financial entities, and bar association ethical rules for law firms. Pre-incident legal counsel review of these obligations — and pre-agreed escalation paths — can substantially improve an organization's ability to respond decisively within the three-day extortion window.

CSA Resource Alignment

The UNC3753 campaign is a direct demonstration of why identity verification, access control, and human-layer security cannot be treated as solved problems in the modern threat landscape. CSA's Zero Trust guidance is directly applicable: the core principle of "never trust, always verify" extends explicitly to inbound IT support interactions, not only to network traffic. The assumption that a caller who knows internal terminology and references real business processes is legitimate is precisely the trust model that UNC3753 exploits. Zero Trust implementations must encompass identity verification for all support interactions, including inbound phone and screen-sharing requests.

The CSA Cloud Controls Matrix (CCM) v4.0 provides specific control domains relevant to this campaign. The Identity and Access Management (IAM) domain — particularly controls IAM-02 (Strong Authentication), IAM-04 (Separation of Duties), and IAM-09 (User Access Authorization) — directly addresses the conditional access gaps that enable the BYOD VDI pivot. The Physical and Environmental Security (PES) domain, including PES-01 through PES-04, speaks to the visitor management and escort

requirements that would mitigate physical intrusion attempts. The Security Incident Management, E-Discovery, and Cloud Forensics (SEF) domain provides the framework for ensuring incident response plans cover the data-theft-only extortion scenario.

CSA's STAR (Security Trust Assurance and Risk) program, and the STAR Registry specifically, enables organizations to assess third-party cloud and SaaS vendors' security postures. Given UNC3753's specific targeting of iManage — a cloud-hosted or hybrid document management platform — organizations should verify that their iManage deployment includes the activity logging, bulk-download alerting, and MFA enforcement that Mandiant's mitigations recommend. STAR assessments of any document management or collaboration platform used to store privileged client data should include explicit evaluation of anomalous access detection capabilities.

The CSA AI Controls Matrix (AICM) is increasingly relevant as law firms and financial services organizations adopt AI-assisted document review, contract analysis, and client communication tools. AI platforms that have access to the same document repositories UNC3753 targets — iManage files, OneDrive folders, email archives — represent an expansion of the attack surface if AI service accounts are not subject to the same access controls, MFA requirements, and activity monitoring as human user accounts. AICM's controls around AI system access governance should be evaluated for all AI tools with access to privileged document stores.

References

[1] Federal Bureau of Investigation. "Silent Ransom Group Impersonating IT Personnel through Social Engineering." IC3 FLASH-20260526-01, May 26, 2026.

[2] Google Cloud / Mandiant Threat Intelligence Group. "Ongoing Targeted Campaign Against US Law Firms." Google Cloud Blog, June 2026.

[3] TechTimes. "Silent Ransom Group Sends Operatives Into Law Firm Offices: 38 Firms Already Leaked." May 27, 2026.

[4] American Hospital Association. "FBI Flash Report TLP Clear: Silent Ransom Group Impersonating IT Personnel through Social Engineering." May 26, 2026.

[5] DataBreaches.Net. "Silent Ransom Group leaked another big law firm: Orrick, Herrington & Sutcliffe." April 10, 2026.

[6] Resecurity. "Silent Ransom Group (SRG): Uncovering DNS Fast Flux Infrastructure." Resecurity Blog, 2026.

