INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-07 18:29 UTC

Silent Ransom Group Escalates Legal Sector Targeting: Vishing, Physical Access, and Sub-30-Minute Extortion

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0422
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft Teams, Zoom, Quick Assist, Microsoft Terminal Services, AnyDesk, Zoho Assist, Bomgar, SuperOps, WinSCP, Rclone, Privnote, targeted across U.S. law firms and professional services organizations
Published	2026-06-07T10:09:19
Discovery Source	Rss

Executive Summary

Silent Ransom Group (also tracked as Luna Moth, UNC3753, and Chatty Spider) is actively targeting U.S. law firms and professional services organizations using phone-based social engineering, legitimate remote access tools, and, in a significant escalation, reported physical presence at victim sites to steal data. Mandiant and the FBI have both issued warnings documenting intrusion timelines as short as 30 minutes from initial contact to exfiltration. The business risk is severe: client data, privileged legal communications, and case files are being stolen and held for extortion without any ransomware deployment, leaving no encryption-based warning signs.

Technical Analysis

Silent Ransom Group (UNC3753 / Luna Moth / Chatty Spider) operates a pure data-theft extortion model with no encryption component, reducing forensic artifacts and shortening time-to-impact. Initial access is gained via callback phishing (T1566.004 / T1598.004), victims receive fraudulent invoices or IT support notifications and are directed to call attacker-controlled numbers. Operators then social-engineer victims into installing legitimate RMM tools: Quick Assist, AnyDesk, Zoho Assist, Bomgar, and SuperOps (T1219). These tools provide persistent remote access abused for lateral movement and data collection. In recent intrusions, operators have been observed physically present at victim office locations during data exfiltration operations, reducing reliance on remote access tools for final data collection stages. Credentials are harvested via social engineering

(CWE-287) and UI overlay/redress techniques (CWE-1021). Fast-flux residential proxy infrastructure (T1090.003, T1568.001) is used to evade IP-based detection and attribution. Data exfiltration occurs via WinSCP and Rclone (T1048, T1567) targeting repositories, shared drives, and document stores (T1213). Extortion demands are communicated via Privnote ephemeral messages (T1657). Internal spearphishing (T1534) has been observed post-compromise for lateral spread. Infrastructure acquisition for operations is tracked under T1583.001. CWE mappings include CWE-284 (improper access control via abused legitimate tools), CWE-693 (protection mechanism failure, security tooling bypassed via trusted RMM), and CWE-287 (improper authentication via social engineering). No CVE applies; the attack chain exploits legitimate software and human trust, not software vulnerabilities. No patch resolves this threat, detection and policy controls are the primary mitigations.

Action Checklist

1. Step 1: Containment. Immediately audit all active RMM tool sessions across the environment. Identify and terminate any unauthorized Quick Assist, AnyDesk, Zoho Assist, Bomgar, or SuperOps sessions. Block outbound connections to RMM tool relay infrastructure at the perimeter if these tools are not sanctioned. Reference CIS 4.4 (Implement and Manage a Firewall on Servers) and CIS 4.5 (Implement and Manage a Firewall on End-User Devices) to enforce default-deny outbound rules for unsanctioned remote access tools. Review building access logs and security camera footage for the intrusion window; verify that all remote access sessions correspond to verified IT staff or contractors. Coordinate with physical security to audit visitor sign-in procedures and badge access records.
2. Step 2: Detection. Query endpoint and network logs for execution of Quick Assist (quickassist.exe), AnyDesk (anydesk.exe), Zoho Assist, Bomgar, and SuperOps processes on endpoints where IT helpdesk activity was not ticketed. Search for WinSCP (winscp.exe) and Rclone (rclone.exe) execution events, particularly with command-line arguments referencing cloud storage endpoints. Review DNS and proxy logs for fast-flux domains (high TTL variance, residential IP resolutions). Audit AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting) compliance, verify these process execution events are captured. Flag inbound calls to help desk queues followed within 30 minutes by RMM tool installation on the caller's endpoint.
3. Step 3: Eradication. Remove all unsanctioned RMM tools from endpoints via software inventory review per CIS 2.3 (Address Unauthorized Software). Enforce application allowlisting to block unauthorized RMM tool execution. Revoke any accounts accessed during suspected sessions and rotate credentials per D3-CRO (Credential Rotation). Enforce CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), standard users must not be able to install RMM tools without IT authorization. Apply NIST AC-6 (Least Privilege) to limit the blast radius of any compromised session.
4. Step 4: Recovery. Validate that all RMM tool installations are inventoried and authorized against CIS 2.1 (Establish and Maintain a Software Inventory). Confirm AU-9 (Protection of Audit Information) controls are intact, verify attacker activity did not tamper with logs. Re-authenticate all accounts that were active during the suspected intrusion window. Monitor outbound data flows via WinSCP and Rclone signatures for 30 days post-remediation. Validate that fast-flux proxy IPs identified during investigation are blocked at the perimeter.
5. Step 5: Post-Incident. Conduct targeted vishing simulation training focused on fake IT support call scenarios, specifically targeting legal and administrative staff. Implement a verified callback policy: IT helpdesk requests to install remote access tools must be confirmed via a second channel before execution. Map control gaps against NIST AC-17 (Remote Access), establish documented usage

restrictions for all remote access tools. Enforce CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access) to reduce the value of socially engineered credentials.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to outside counsel and executive leadership if any client confidential data, privileged communications, or personally identifiable information was accessible on systems touched during the Silent Ransom Group session — law firms face attorney-client privilege breach exposure and state breach notification obligations that may trigger within 30-72 hours of discovery, and the FBI has issued an active warning on this campaign warranting law enforcement notification.
Recovery Notes	Given Silent Ransom Group's documented sub-30-minute exfiltration capability using Rclone and WinSCP to cloud storage destinations, assume data exfiltration occurred on any endpoint where these tools executed and scope the breach accordingly before clearing systems for return to production. Monitor all previously compromised endpoints for 30 days post-remediation using Sysmon Event ID 3 (NetworkConnect) alerts on Rclone and WinSCP process names, and maintain perimeter blocks on fast-flux IPs and cloud storage destinations observed during the incident. Verify that Microsoft Teams and Zoom tenant-level audit logging is enabled and retained for a minimum of 90 days before returning to normal operations, as these platforms are Silent Ransom Group's primary initial access vectors and must be instrumented for future detection.
Forensic Artifacts	Sysmon Event ID 1 (Process Create) logs for anydesk.exe, quickassist.exe, rclone.exe, winscp.exe — CommandLine field will contain cloud storage endpoint arguments and file paths targeted for exfiltration, directly evidencing Silent Ransom Group's data theft activity | Microsoft Teams application log at %AppData%\Microsoft\Teams\logs.txt and Zoom logs at %AppData%\Zoom\logs — will contain records of file transfers used by Silent Ransom Group to deliver RMM tool installers to victims under the guise of IT support | Rclone configuration file at %AppData%\rclone\rclone.conf and WinSCP session file at %AppData%\WinSCP\WinSCP.ini — will contain attacker-configured cloud storage destination credentials and transfer history, identifying exfiltration targets | Windows Prefetch files at C:\Windows\Prefetch\RCLONE.EXE-*.pf and ANYDESK.EXE-*.pf — provide forensic proof of execution including run count and last execution timestamp even if binaries were deleted by the operator post-exfiltration | Phone system Call Detail Records (CDR) for inbound calls to the help desk queue — correlating call timestamps with RMM process creation events (Sysmon Event ID 1) will establish the vishing-to-installation timeline and confirm Silent Ransom Group's social engineering vector for this specific incident

Per-Action IR Details

Step 1: Containment — Immediately audit all active RMM tool sessions across the environment. Identify and terminate any unauthorized Quick Assist, AnyDesk, Zoho Assist, Bomgar, or SuperOps sessions. Block outbound connections to RMM tool relay infrastructure at the perimeter if these tools are not sanctioned. Reference CIS 4.4 (Implement and Manage a Firewall on Servers) and CIS 4.5 (Implement and Manage a Firewall on End-User Devices) to enforce default-deny outbound rules for unsanctioned remote access tools.

NIST Phase: Containment

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

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

Compensating: On Windows endpoints without EDR, run: `Get-Process | Where-Object {$_.Name -match 'quickassist|anydesk|zohoassist|bomgar|superops'} | Select-Object Name, Id, StartTime` to identify live RMM processes, then terminate with `Stop-Process -Id -Force`. At the perimeter firewall or Windows host firewall, block outbound TCP to known AnyDesk relay ranges (193.34.166.0/24) and Quick Assist relay (*.remoteassistance.microsoft.com) using `netsh advfirewall firewall add rule` if AnyDesk/Quick Assist are unsanctioned. On Linux gateways, use `iptables -A OUTPUT -p tcp --dport 443 -d -j DROP` for Rclone and WinSCP cloud egress CIDRs (e.g., AWS S3, Mega.nz).

Evidence: Before terminating sessions: capture full process tree from Task Manager or `Get-CimInstance Win32_Process | Select-Object Name,ProcessId,ParentProcessId,CommandLine` to document parent-child relationships (e.g., Teams or Zoom spawning anydesk.exe). Screenshot or export active network connections via `netstat -anob > connections_precontainment.txt` to preserve relay IP and port. Capture Windows Event Log — Security Event ID 4688 (Process Creation) with command-line auditing enabled — filtered for quickassist.exe, anydesk.exe, rclone.exe, winscp.exe in the 60-minute window prior to containment. Export raw EVTX files before any remediation activity.

Step 2: Detection — Query endpoint and network logs for execution of Quick Assist (quickassist.exe), AnyDesk (anydesk.exe), Zoho Assist, Bomgar, and SuperOps processes on endpoints where IT helpdesk activity was not ticketed. Search for WinSCP (winscp.exe) and Rclone (rclone.exe) execution events, particularly with command-line arguments referencing cloud storage endpoints. Review DNS and proxy logs for fast-flux domains (high TTL variance, residential IP resolutions). Audit AU-2 (Event Logging) and AU-6 (Audit Record Review, Analysis, and Reporting) compliance — verify these process execution events are captured. Flag inbound calls to help desk queues followed within 30 minutes by RMM tool installation on the caller's endpoint.

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), NIST AU-3 (Content Of Audit Records)

Compensating: Deploy Sysmon with SwiftOnSecurity config (minimum: ProcessCreate Event ID 1, NetworkConnect Event ID 3) — filter on Image path matching anydesk.exe, rclone.exe, winscp.exe. Query Sysmon Event ID 1 logs using: `Get-WinEvent -LogName 'Microsoft-Windows-Sysmon/Operational' | Where-Object {$_.Message -match 'rclone|winscp|anydesk|quickassist'} | Select-Object TimeCreated,Message`. For DNS fast-flux detection without SIEM, use osquery: `SELECT name, type, answer FROM dns_resolvers` combined with manual review of Windows DNS cache (`ipconfig /displaydns`) for domains with TTL under 300 seconds resolving to residential IP blocks. Cross-reference help desk call logs (phone system CDR exports) against endpoint process creation timestamps — a Silent Ransom Group intrusion window is documented at under 30 minutes, so correlate call start time ± 30 minutes against RMM executable first-seen timestamps.

Evidence: Sysmon Event ID 1 (Process Create) for anydesk.exe, quickassist.exe, rclone.exe, winscp.exe — capture full CommandLine field, which for Rclone will contain cloud storage endpoint arguments (e.g., `rclone copy C:\mega:exfil` or `rclone sync --transfers 32 C:\Users\\Documents dropbox:dump`). Windows Security Event ID 4624/4625 (Logon Success/Failure) for accounts active during the vishing call window. Microsoft Teams or Zoom application logs (located at `%AppData%\Microsoft\Teams\logs.txt` and `%AppData%\Zoom\logs`) to identify whether the initial social engineering contact was made via those platforms before RMM tool deployment. Proxy/DNS logs showing resolution of Privnote domains (privnote.com) used by Silent Ransom Group for self-destructing communication, and any anomalous FQDN with TTL variance greater than 50% between consecutive lookups.

Step 3: Eradication — Remove all unsanctioned RMM tools from endpoints via software inventory review per CIS 2.3 (Address Unauthorized Software). Enforce application allowlisting to block unauthorized RMM tool execution. Revoke any accounts accessed during suspected sessions and rotate credentials per D3-CRO (Credential Rotation). Enforce CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

— standard users must not be able to install RMM tools without IT authorization. Apply NIST AC-6 (Least Privilege) to limit the blast radius of any compromised session.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: CIS 2.3 (Address Unauthorized Software), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), NIST AC-6 (Least Privilege), NIST AC-2 (Account Management)

Compensating: Use `wmic product where 'name like "%AnyDesk%" or name like "%Zoho%" or name like "%BeyondTrust%"' call uninstall /nointeractive` to remove unsanctioned RMM tools at scale via script. For application allowlisting without enterprise tooling, enable Windows Software Restriction Policies or AppLocker (available on Win10 Pro/Enterprise) — create a rule set that denies execution from `%TEMP%`, `%APPDATA%`, and user-writable paths where Silent Ransom Group typically stages RMM installers dropped via Teams/Zoom file transfer. Rotate credentials for all accounts whose sessions were observed in Event ID 4624 logs during the intrusion window using: `net user /domain`. Purge Rclone configuration files at `%APPDATA% clone clone.conf` which may contain persisted cloud storage credentials.

Evidence: Before uninstalling RMM tools: capture installer artifacts from `%TEMP%`, `%Downloads%`, and `%AppData%\Local\Temp` — Silent Ransom Group delivers RMM installers via Teams or Zoom file share, so collect file metadata (hash, creation timestamp, originating process) using `Get-FileHash -Algorithm SHA256` and `Get-Item | Select-Object Name,CreationTime,LastWriteTime`. Export Rclone config at `%APPDATA% clone clone.conf` and WinSCP session logs at `%APPDATA%\WinSCP\WinSCP.ini` before deletion — these will contain cloud exfiltration destination addresses and potentially authentication tokens. Capture Windows Prefetch files (`C:\Windows\Prefetch\RCLONE.EXE-*.pf`) as evidence of execution even if binary has been deleted.

Step 4: Recovery — Validate that all RMM tool installations are inventoried and authorized against CIS 2.1 (Establish and Maintain a Software Inventory). Confirm AU-9 (Protection of Audit Information) controls are intact — verify attacker activity did not tamper with logs. Re-authenticate all accounts that were active during the suspected intrusion window. Monitor outbound data flows via WinSCP and Rclone signatures for 30 days post-remediation. Validate that fast-flux proxy IPs identified during investigation are blocked at the perimeter.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: CIS 2.1 (Establish and Maintain a Software Inventory), NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), NIST AC-12 (Session Termination)

Compensating: Use osquery to generate a live software inventory across all endpoints: `SELECT name, version, install_date FROM programs WHERE name LIKE '%assist%' OR name LIKE '%AnyDesk%' OR name LIKE '%rclone%'` — diff output against your authorized software baseline. Verify log integrity by checking Windows Security Event Log for Event ID 1102 (Audit Log Cleared) or Event ID 104 (System Log Cleared) — Silent Ransom Group operators have been observed attempting log suppression post-exfiltration. For 30-day monitoring without SIEM, deploy a Sigma rule converted to Windows Event Log queries targeting Rclone and WinSCP network signatures: monitor Sysmon Event ID 3 (NetworkConnect) for destination ports 22 (SFTP/WinSCP) and 443 with process name rclone.exe. Block fast-flux IPs identified during investigation using Windows Firewall GPO or perimeter ACL — retain the block list as documented evidence.

Evidence: Validate log chain of custody: export and hash (SHA-256) all EVTX files from the Security, System, and Application channels covering the intrusion window before any system changes — compare against any centralized log copies to detect tampering. Check `%SystemRoot%\System32\winevt\Logs\` for last-modified timestamps inconsistent with normal log rotation, which may indicate manual clearing by the Silent Ransom Group operator. Review Microsoft Teams and Zoom application audit logs (if tenant-level logging was enabled) for file transfer records — these will document the exact filenames and sizes of RMM installers delivered to victims, supporting data breach scope assessment for law firm client-privilege notifications.

Step 5: Post-Incident — Conduct targeted vishing simulation training focused on fake IT support call scenarios, specifically targeting legal and administrative staff. Implement a verified callback policy: IT helpdesk requests to install remote access tools must be confirmed via a second channel before execution.

Map control gaps against NIST AC-17 (Remote Access) — establish documented usage restrictions for all remote access tools. Enforce CIS 6.3 (Require MFA for Externally-Exposed Applications) and CIS 6.5 (Require MFA for Administrative Access) to reduce the value of socially engineered credentials. Brief physical security teams on the reported physical site access tactic and review visitor control procedures.

NIST Phase: Post Incident

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

Controls: NIST AC-17 (Remote Access), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process), NIST AU-6 (Audit Record Review, Analysis, And Reporting)

Compensating: For vishing simulation without a commercial platform, draft a tabletop scenario script mimicking Silent Ransom Group's documented pretext — caller claims to be IT helpdesk responding to a subscription cancellation alert (their known lure), requests Teams screen share, then asks to install AnyDesk. Run the scenario with legal and administrative staff quarterly. For the verified callback policy, document a one-page procedure: any unsolicited helpdesk call requesting remote tool installation must be terminated, and the staff member must call back the IT helpdesk using the number listed on the internal intranet (not one provided by the caller). For physical access controls, implement a visitor log with photo ID requirement and escort policy — cross-reference visitor logs against the intrusion timeline as part of this post-incident review to determine whether physical presence at the law firm site is confirmed.

Evidence: Compile a lessons-learned report documenting the full Silent Ransom Group intrusion timeline — from initial vishing call timestamp (sourced from phone system CDR) through RMM tool installation (Sysmon Event ID 1 timestamp) to exfiltration completion (last Rclone/WinSCP network connection in Sysmon Event ID 3) — to validate whether the sub-30-minute window documented by Mandiant and the FBI applied to this incident. Preserve all Privnote URLs or self-destructing message links observed during the incident as indicators, and submit to CISA's Malware Next-Gen Analysis portal and your sector ISAC (FS-ISAC or equivalent legal sector group) for threat intelligence sharing.

Detection Guidance

Primary behavioral indicators: (1) Execution of Quick Assist (quickassist.exe), AnyDesk (anydesk.exe), Zoho Assist, Bomgar, or SuperOps on endpoints with no corresponding IT helpdesk ticket, query endpoint telemetry for process creation events for these executables within 30 minutes of any help desk call record. (2) WinSCP or Rclone execution with command-line arguments pointing to external cloud or SFTP destinations, these tools have no legitimate business justification on legal workstations in most environments. (3) DNS resolution patterns showing rapid IP rotation on domains associated with RMM tool relay servers or extortion infrastructure (fast-flux indicators: TTL under 300 seconds, multiple A records resolving to residential IP ranges). (4) Outbound data volume anomalies on workstations during or after RMM tool sessions, large file transfers via WinSCP or Rclone will produce elevated upload traffic spikes. (5) Privnote-related outbound connections (privnote.com) from workstations during or after suspected sessions. (6) Internal spearphishing indicators: emails sent from a compromised internal account to colleagues containing links or attachments inconsistent with normal communication patterns (T1534). Log sources to prioritize: EDR process creation and network connection logs, DNS query logs, proxy/firewall outbound logs, email gateway logs for internal-to-internal anomalies. Reference AU-2 (Event Logging) and AU-12 (Audit Record Generation) to confirm these event types are captured. CIS 8.2 (Collect Audit Logs) compliance is a prerequisite, environments not logging process execution will have no forensic visibility into this attack chain.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`privnote.com`	Legitimate ephemeral messaging service abused by Silent Ransom Group to deliver extortion demands; outbound connections from corporate endpoints to this domain during or after an RMM session are a high-confidence indicator	MEDIUM
URL	`No confirmed IOC URLs available in source data — see FBI and Mandiant advisories for current infrastructure indicators`	Fast-flux residential proxy infrastructure is used; specific IPs and domains rotate rapidly and are not reliably static. Consumers should obtain current IOC feeds from FBI IC3 and Mandiant directly.	LOW

Framework Mappings

MITRE-ATTACK

- **T1071** — Application Layer Protocol
- **T1567** — Exfiltration Over Web Service
- **T1090.003** — Multi-hop Proxy
- **T1078** — Valid Accounts
- **T1568.001** — Fast Flux DNS
- **T1105** — Ingress Tool Transfer
- **T1583.001** — Domains
- **T1598.004** — Spearphishing Voice
- **T1048** — Exfiltration Over Alternative Protocol
- **T1560** — Archive Collected Data
- **T1534** — Internal Spearphishing
- **T1566.004** — Spearphishing Voice
- **T1219** — Remote Access Tools
- **T1213** — Data from Information Repositories
- **T1657** — Financial Theft

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management

- **SI-3** — Malicious Code Protection
- **AC-3** — Access Enforcement
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **CP-9** — System Backup
- **IR-4** — Incident Handling
- **AT-2** — Literacy Training and Awareness
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

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

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(7)(ii)(A)** — Data Backup Plan
- **164.308(a)(5)(i)** — Security Awareness and Training
- **164.308(a)(6)(ii)** — Response and Reporting
- **164.312(e)(1)** — Transmission Security

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

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
T1071	Application Layer Protocol	Command-And-Control
T1567	Exfiltration Over Web Service	Exfiltration
T1090.003	Multi-hop Proxy	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1568.001	Fast Flux DNS	Command-And-Control
T1105	Ingress Tool Transfer	Command-And-Control
T1583.001	Domains	Resource-Development
T1598.004	Spearphishing Voice	Reconnaissance
T1048	Exfiltration Over Alternative Protocol	Exfiltration
T1560	Archive Collected Data	Collection
T1534	Internal Spearphishing	Lateral-Movement
T1566.004	Spearphishing Voice	Initial-Access
T1219	Remote Access Tools	Command-And-Control
T1213	Data from Information Repositories	Collection
T1657	Financial Theft	Impact

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/silent-ransom-group-...	T3
Solve PC problems remotely using Quick Assist - Microsoft Support	https://support.microsoft.com/en-us/windows/solve-pc-problems-remot...	T1
Remote Assistance Tools? : r/sysadmin - Reddit	https://www.reddit.com/r/sysadmin/comments/1oqz22k/remote_assistanc...	T3
Microsoft Quick Assist Remote Monitoring - Inversion6	https://inversion6.com/insights/blog/microsoft-quick-assist-an-it-s...	T3

Source	URL	Tier
Teams Social Engineering Attack: Threat Actors Impersonate IT to ...	https://www.cyberproof.com/blog/teams-social-engineering-attack-thr...	T3

Generated 2026-06-07 18:29 UTC by TJS Security Command Center