INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-08 13:48 UTC

UNC3753 Completes Full Extortion Cycle in Under a Day, Physical Intrusions Now Confirm Multi-Vector Escalation

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0425
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	AnyDesk, Bomgar, SuperOps RMM, Zoho Assist, Zoom, Microsoft Teams, Quick Assist, WinSCP, Rclone, corporate VDI environments
Published	2026-06-08T03:39:28
Discovery Source	Rss

Executive Summary

UNC3753 (also tracked as Luna Moth and Silent Ransom Group) is conducting targeted extortion campaigns against U.S. professional, legal, and financial services firms, completing the full cycle from initial contact to data theft and extortion demand within a single business day. The group bypasses all technical controls entirely through social engineering: employees are manipulated via phone calls and Microsoft Teams or Zoom impersonation into installing legitimate remote access tools, after which data is staged and exfiltrated. A confirmed escalation to in-person physical intrusion by actors posing as IT technicians marks a significant expansion in threat capability and raises the risk profile for any organization with shared office environments or third-party IT support relationships.

Technical Analysis

UNC3753 operates without exploiting CVEs. The attack chain relies exclusively on vishing (T1566.004, T1598), cross-tenant impersonation via Microsoft Teams and Zoom (T1656), and manipulation of employees into installing legitimate RMM tools: AnyDesk, Bomgar, SuperOps RMM, and Zoho Assist (T1219, T1204.002). Once remote access is established, operators conduct lateral movement, data discovery (T1213), and staging (T1560) before exfiltrating via WinSCP and Rclone (T1048, T1071, T1567). Valid accounts are leveraged throughout (T1078). Infrastructure uses fast-flux DNS distributed across 18 countries (T1583.001), reducing the efficacy of domain-based blocking strategies. Physical intrusion by actors posing as IT technicians has been confirmed (T1200), representing a multi-vector capability expansion. No patch applies. Applicable CWEs are CWE-693

(Protection Mechanism Failure) and CWE-1021 (Improper Restriction of Rendered UI Layers), reflecting wholesale bypass of security controls through trust manipulation rather than technical exploitation. Primary source: Microsoft Security Blog, Cross-Tenant Helpdesk Impersonation to Data Exfiltration (T1 source, 2026-04-18).

Action Checklist

1. Step 1: Containment, Block or place under monitoring all unsanctioned RMM tool installations organization-wide. Audit active AnyDesk, Bomgar, SuperOps RMM, and Zoho Assist sessions immediately; terminate any sessions not initiated through a documented IT change ticket. Restrict Quick Assist and Teams remote control features via Group Policy or Intune to authorized IT accounts only. Enforce CIS 2.3: remove or quarantine unauthorized software on all enterprise assets.
2. Step 2: Detection, Query EDR and endpoint logs for execution of AnyDesk.exe, BomgarConsole.exe, SuperOps agent installers, ZohoAssist.exe, rclone.exe, and WinSCP.exe outside of authorized software inventory (CIS 2.1). Review Microsoft Teams external access logs for inbound messages from external or cross-tenant accounts impersonating IT helpdesk personas. Alert on bulk file access, staging to unusual directories, and outbound transfers via cloud storage endpoints or SFTP. Enable NIST AU-2 event logging across endpoint and identity platforms to capture RMM installation events, authentication anomalies, and lateral movement indicators.
3. Step 3: Eradication & Hardening, Since there is no patch, eradication requires thorough removal of unauthorized RMM agents from all endpoints, followed by policy enforcement to prevent reinfection. Enforce application allowlisting to restrict RMM tool installation to authorized IT accounts only (CIS 2.3, CIS 4.6). Disable or block Teams external access and cross-tenant communication where not operationally required. Require all remote support sessions to originate from ticketed IT requests verified through a secondary out-of-band channel. Enforce NIST AC-6 (Least Privilege) and AC-3 (Access Enforcement) to prevent unauthorized lateral movement after initial access.
4. Step 4: Recovery, Validate that all unauthorized RMM sessions are terminated and that no persistent agents remain on endpoints. Rotate credentials for any account that received a vishing call or installed an RMM tool, per D3-CRO (Credential Rotation). Audit VDI environment access logs for anomalous session activity. Verify MFA enrollment status for all externally-exposed applications (CIS 6.3) and remote access paths (CIS 6.4). Monitor exfiltration-relevant egress paths (Rclone, WinSCP, cloud storage) for 30 days post-incident.
5. Step 5: Post-Incident, This campaign exposed gaps in human-layer controls and physical access verification. Implement a mandatory callback verification protocol: any employee receiving an unsolicited IT support call must verify the request through a separately published IT helpdesk number before granting remote access. Deliver targeted security awareness training focused on vishing, IT impersonation, and physical access verification. Review physical access controls for shared office and data center environments. Map control gaps to NIST AC-17 (Remote Access), AC-20 (Use of External Systems), and CIS 5.4 (Restrict Administrator Privileges). No mapped control covers in-person physical intrusion detection within the loaded knowledge base; a physical security review is warranted outside these frameworks.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if forensic evidence confirms exfiltration of client PII, privileged legal communications, or financial records from professional services environments — triggering state breach notification obligations and potential SEC or FTC reporting requirements — or if physical intrusion into a data center or secure area is confirmed, indicating capability beyond remote-only attack chains.
Recovery Notes	Before declaring recovery, verify via osquery and Windows Services enumeration that no UNC3753-installed RMM agent (AnyDesk, Bomgar, SuperOps, ZohoAssist) persists as a running service or scheduled task on any endpoint that received a vishing call, as the group is known to establish persistent access quickly after initial installation. Audit all VDI session logs and M365 Unified Audit Logs for the 48 hours surrounding the incident to identify any lateral movement or secondary access establishment that occurred before containment. Maintain enhanced egress monitoring on Rclone, WinSCP, and cloud storage endpoints (Backblaze B2, Mega.nz, AWS S3, SFTP destinations) for a minimum of 30 days, as UNC3753 has demonstrated staged exfiltration behavior where initial transfers are followed by secondary collection attempts after defenders stand down.
Forensic Artifacts	AnyDesk session trace files at `%AppData%\AnyDesk\ad_svc.trace` and `%AppData%\AnyDesk\connection_trace.txt` — contain remote operator IP addresses, session start/end timestamps, and file transfer events specific to the UNC3753 operator-controlled AnyDesk ID | Windows Prefetch files `C:\Windows\Prefetch\RCLONE.EXE-*.pf` and `WINSCP.EXE-*.pf` — confirm execution timestamps, run counts, and directory paths accessed during UNC3753 staging and exfiltration activity even after binaries are deleted | Microsoft Teams Unified Audit Log (M365 Compliance Center) — Operations `ChatMessageReceived` and `MessageCreatedHasLink` from external or federated tenant accounts with display names impersonating IT helpdesk, constituting the primary social engineering delivery record for this campaign | ShimCache (AppCompatCache) at `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache` and AmCache at `C:\Windows\appcompat\Programs\Amcache.hve` — evidence of RMM binary execution history on endpoints where Prefetch is disabled, covering all four RMM tools used by UNC3753 | Windows Security Event ID 4663 (File System Object Access) on file servers — sequential high-volume read events from a single compromised user account in a compressed timeframe, identifying the specific files staged by UNC3753 prior to Rclone or WinSCP exfiltration

Per-Action IR Details

Step 1: Containment — Block or place under monitoring all unsanctioned RMM tool installations organization-wide. Audit active AnyDesk, Bomgar, SuperOps RMM, and Zoho Assist sessions immediately; terminate any sessions not initiated through a documented IT change ticket. Restrict Quick Assist and Teams remote control features via Group Policy or Intune to authorized IT accounts only. Enforce CIS 2.3: remove or quarantine unauthorized software on all enterprise assets.

NIST Phase: Containment

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

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), CIS 2.3 (Address Unauthorized Software), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

Compensating: Use PowerShell across endpoints to identify active RMM processes: `Get-Process | Where-Object {$_.Name -match 'AnyDesk|BomgarConsole|ZohoAssist|superops'}`. Kill unauthorized sessions via `Stop-Process

-Name AnyDesk -Force`. Deploy a Sysmon configuration (SwiftOnSecurity baseline) with Event ID 1 (Process Create) filtering on those binary names to flag re-launch attempts. Use Windows Firewall GPO to block outbound TCP 7070 (AnyDesk default), 443 to known Bomgar relay domains, and ZohoAssist cloud relay IPs at the host level without requiring a SIEM.

Evidence: Before terminating sessions, capture: AnyDesk session logs at `%AppData%\AnyDesk\ad_svc.trace` and `%AppData%\AnyDesk\connection_trace.txt` (contain remote IP, session timestamps, and file transfer events); ZohoAssist session records from `%ProgramData%\ZohoMeeting\logs`; Bomgar session logs from the local representative console cache; Windows Event Log Security channel Event ID 4688 (Process Creation) for the parent-child chain showing which user account launched the RMM installer; Intune or SCCM device compliance snapshots prior to any remediation push.

Step 2: Detection — Query EDR and endpoint logs for execution of AnyDesk.exe, BomgarConsole.exe, SuperOps agent installers, ZohoAssist.exe, rclone.exe, and WinSCP.exe outside of authorized software inventory (CIS 2.1). Review Microsoft Teams external access logs for inbound messages from external or cross-tenant accounts impersonating IT helpdesk personas. Alert on bulk file access, staging to unusual directories, and outbound transfers via cloud storage endpoints or SFTP. Enable NIST AU-2 event logging across endpoint and identity platforms to capture RMM installation events, authentication anomalies, and lateral movement indicators.

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), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 8.2 (Collect Audit Logs)

Compensating: Without EDR, deploy Sysmon with Event ID 1 filtering for `rclone.exe`, `WinSCP.exe`, and all four RMM binaries by image name and hash. Use osquery with query `SELECT name, path, pid, cmdline FROM processes WHERE name IN ('rclone.exe','WinSCP.exe','AnyDesk.exe','ZohoAssist.exe','BomgarConsole.exe');` scheduled every 5 minutes. For Teams external access, pull the Microsoft 365 Unified Audit Log via PowerShell: `Search-UnifiedAuditLog -RecordType MicrosoftTeams -Operations MessageCreatedHasLink` and filter on `CommunicationType eq 'OneOnOne'` from external tenants. Use Wireshark or Windows packet capture (`netsh trace start`) to flag outbound SFTP (TCP 22) or Rclone-to-cloud (TCP 443 to known cloud storage ASNs) from non-server endpoints.

Evidence: Microsoft Teams Unified Audit Log entries (Operations: `ChatMessageReceived`, `MessageCreatedHasLink`) showing external or federated sender UPNs with display names mimicking internal IT helpdesk (e.g., 'IT Support', 'HelpDesk-Tier2'); Windows Security Event ID 4688 process creation records showing `rclone.exe` or `WinSCP.exe` launched from user-writable directories such as `%TEMP%` or `%USERPROFILE%\Downloads`; Sysmon Event ID 3 (Network Connection) for outbound connections from `rclone.exe` to cloud storage endpoints (Backblaze B2, Mega.nz, AWS S3); Windows Security Event ID 4663 (File System Object Access) on file server shares showing high-volume sequential read access from a single user account within a compressed timeframe, characteristic of UNC3753 staging prior to exfiltration.

Step 3: Eradication — There is no patch. Eradication requires policy enforcement: restrict RMM tool installation to authorized IT accounts via application allowlisting (CIS 2.3, CIS 4.6). Disable or block Teams external access and cross-tenant communication where not operationally required. Require all remote support sessions to originate from ticketed IT requests verified through a secondary out-of-band channel. Enforce NIST AC-6 (Least Privilege) and AC-3 (Access Enforcement) to prevent unauthorized lateral movement after initial access.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST AC-3 (Access Enforcement), NIST AC-6 (Least Privilege), NIST AC-17 (Remote Access), CIS 2.3 (Address Unauthorized Software), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 4.7 (Manage Default Accounts on Enterprise Assets and Software)

Compensating: Without an enterprise allowlisting platform, use Windows AppLocker (available in Windows 10/11 Pro and Enterprise) with Publisher rules that permit only IT-signed or vendor-signed RMM binaries installed under `%ProgramFiles%`. Block user-writable paths (`%TEMP%`, `%APPDATA%`, `%USERPROFILE%\Downloads`) from executing `.exe` files via AppLocker Executable Rules. Disable Microsoft Teams external access via the Teams Admin Center (Org-wide settings → External Access → toggle off federation for unverified tenants). For cross-tenant impersonation, enable Teams 'External Access allow-list only' mode and whitelist only explicitly trusted partner tenant domains. Script verification: `Get-AppLockerPolicy -Effective -Xml` to confirm rule deployment.

Evidence: Before enforcing AppLocker or removing RMM binaries, collect: full disk image or at minimum a forensic copy of `%APPDATA%`, `%TEMP%`, and `%USERPROFILE%\Downloads` from each compromised endpoint; Windows Prefetch files (`C:\Windows\Prefetch\RCLONE.EXE-*.pf`, `WINSCP.EXE-*.pf`) which confirm execution timestamps and run counts even after binary removal; ShimCache (AppCompatCache) registry key at `HKLM\SYSTEM\CurrentControlSet\Control\Session Manager\AppCompatCache` for evidence of RMM binary execution on systems where Prefetch is disabled; Teams chat export (via M365 Compliance Center Content Search) of the impersonation conversation thread before account or message deletion.

Step 4: Recovery — Validate that all unauthorized RMM sessions are terminated and that no persistent agents remain on endpoints. Rotate credentials for any account that received a vishing call or installed an RMM tool, per D3-CRO (Credential Rotation). Audit VDI environment access logs for anomalous session activity. Verify MFA enrollment status for all externally-exposed applications (CIS 6.3) and remote access paths (CIS 6.4). Monitor exfiltration-relevant egress paths (Rclone, WinSCP, cloud storage) for 30 days post-incident.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AC-2 (Account Management), NIST AC-7 (Unsuccessful Logon Attempts), NIST AC-12 (Session Termination), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access)

Compensating: Validate RMM agent removal with osquery: `SELECT * FROM services WHERE name LIKE '%anydesk%' OR name LIKE '%bomgar%' OR name LIKE '%zohoassist%' OR name LIKE '%superops%';` — any result indicates a persistent service requiring manual removal. For VDI audit without a SIEM, pull Citrix or VMware Horizon session logs for the 72-hour window around the incident and filter for sessions initiated outside business hours or from atypical source IPs. Rotate credentials via scripted AD password reset for affected accounts: `Set-ADAccountPassword -Identity -Reset -NewPassword (ConvertTo-SecureString -AsPlainText '' -Force)` combined with `Revoke-AzureADUserAllRefreshTokens` for M365 sessions. Set up a 30-day Sysmon + Windows Firewall log review cron (Linux) or Scheduled Task (Windows) to alert on re-emergence of Rclone or WinSCP network connections.

Evidence: VDI session broker logs (Citrix StoreFront IIS logs at `C:\inetpub\logs\LogFiles\W3SVC*` or VMware Horizon Connection Server logs at `%ProgramData%\VMware\VDM\logs`) showing session source IPs, authentication timestamps, and virtual desktop assignments for the incident window; Azure AD or on-prem AD authentication logs (Event ID 4624 Logon, Event ID 4648 Explicit Credential Logon) for accounts known to have received vishing calls, to identify lateral movement prior to credential rotation; Network flow data or Windows Firewall logs showing outbound connections from affected endpoints to Rclone-associated cloud storage endpoints or WinSCP SFTP destinations, to confirm scope of data exfiltration before declaring recovery complete.

Step 5: Post-Incident — This campaign exposed gaps in human-layer controls and physical access verification. Implement a mandatory callback verification protocol: any employee receiving an unsolicited IT support call must verify the request through a separately published IT helpdesk number before granting remote access. Deliver targeted security awareness training focused on vishing, IT impersonation, and physical access verification. Review physical access controls for shared office and data center environments. Map control gaps to NIST AC-17 (Remote Access), AC-20 (Use of External Systems), and CIS 5.4 (Restrict Administrator Privileges). No mapped control covers in-person physical intrusion detection within the loaded knowledge base — a physical security review is warranted outside these frameworks.

NIST Phase: Post Incident

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

Controls: NIST AC-17 (Remote Access), NIST AC-20 (Use Of External Systems), NIST AU-6 (Audit Record Review, Analysis, And Reporting), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.1 (Establish an Access Granting Process), CIS 6.2 (Establish an Access Revoking Process), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Callback verification protocol requires zero budget: publish a laminated IT helpdesk callback card at every employee workstation and include the verified number in the email signature footer of all IT staff. For vishing-specific awareness training, use CISA's free 'Phishing Guidance' materials and adapt scenarios to Teams and Zoom impersonation of internal IT personas — the exact UNC3753 delivery vector. For physical access gap analysis, conduct a tabletop exercise (no tooling required) simulating an actor tailgating into a shared office space and requesting local workstation access under an IT pretext. Document findings and track remediation in a shared spreadsheet mapped to the control gaps identified in this incident for the next audit cycle.

Evidence: Physical access badge logs from the building management system for the incident date and time window, cross-referenced against employee schedules to identify tailgating or unauthorized entries into secure areas; Microsoft Teams Admin Center external access audit logs retained from the incident period, preserved for regulatory notification requirements if PII or client confidential data from legal or financial services matters was confirmed exfiltrated; Lessons-learned documentation capturing the specific social engineering script used by UNC3753 (reconstructed from employee interviews and Teams chat exports), to be used as the primary training scenario in post-incident awareness sessions.

Detection Guidance

Detection for UNC3753 is behavioral, not signature-based. Key indicators: (1) RMM tool installation (AnyDesk, Bomgar, SuperOps, Zoho Assist) initiated from a standard user account or outside a change management ticket, query EDR process creation logs for these executables with parent processes of web browsers or email clients. (2) Rclone or WinSCP execution followed by outbound transfers to non-corporate destinations, alert on rclone.exe or WinSCP.exe spawning with command-line arguments pointing to external hosts. (3) Microsoft Teams messages originating from external or cross-tenant tenants impersonating IT helpdesk display names, audit Teams external communication logs and detect and flag display name spoofing patterns (e.g., 'IT Help Desk' from an external domain). (4) Bulk file access or directory enumeration events from endpoints that recently ran RMM tools, correlate file access volume spikes with RMM execution timestamps. (5) Authentication events using valid credentials from unusual source IPs or during off-hours, particularly in VDI environments (NIST AU-6). (6) Fast-flux DNS resolution returning multiple short-TTL IPs for the same domain, DNS query logs showing rapid IP rotation for a domain contacted by an RMM process should be treated as high-confidence indicators. Physical intrusion indicators fall outside SIEM scope; recommend reviewing physical access badge logs for any unscheduled IT vendor visits during the January-May 2026 campaign window.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`fast-flux DNS infrastructure across 18 countries — no specific domains confirmed in loaded sources`	UNC3753 uses fast-flux DNS for C2 and RMM callback infrastructure; specific domains not disclosed in available T1/T3 sources	LOW

Type	Value	Context	Confidence
URL	`https://www.microsoft.com/en-us/security/blog/2026/04/18/crosstenant-helpdesk-impersonation-data-exfiltration-human-operated-intrusion-playbook/`	Microsoft T1 source — cross-tenant helpdesk impersonation playbook; may contain additional IOCs not reproduced here	HIGH

Framework Mappings

MITRE-ATTACK

- **T1656** — Impersonation
- **T1567** — Exfiltration Over Web Service
- **T1071** — Application Layer Protocol
- **T1583.001** — Domains
- **T1557** — Adversary-in-the-Middle
- **T1566.004** — Spearphishing Voice
- **T1071.004** — DNS
- **T1048** — Exfiltration Over Alternative Protocol
- **T1219** — Remote Access Tools
- **T1078** — Valid Accounts
- **T1598.004** — Spearphishing Voice
- **T1560** — Archive Collected Data
- **T1204.002** — Malicious File
- **T1213** — Data from Information Repositories
- **T1657** — Financial Theft
- **T1598** — Phishing for Information
- **T1200** — Hardware Additions

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

CIS-V8

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks

HIPAA-SECURITY

- **164.308(a)(6)(ii)** — Response and Reporting

SOC2-TSC

- **CC7.4** — Responds to identified security incidents

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1656	Impersonation	Defense-Evasion
T1567	Exfiltration Over Web Service	Exfiltration
T1071	Application Layer Protocol	Command-And-Control
T1583.001	Domains	Resource-Development
T1557	Adversary-in-the-Middle	Credential-Access
T1566.004	Spearphishing Voice	Initial-Access
T1071.004	DNS	Command-And-Control
T1048	Exfiltration Over Alternative Protocol	Exfiltration
T1219	Remote Access Tools	Command-And-Control
T1078	Valid Accounts	Defense-Evasion
T1598.004	Spearphishing Voice	Reconnaissance
T1560	Archive Collected Data	Collection
T1204.002	Malicious File	Execution
T1213	Data from Information Repositories	Collection
T1657	Financial Theft	Impact
T1598	Phishing for Information	Reconnaissance
T1200	Hardware Additions	Initial-Access

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/06/unc3753-used-vishing-and-physical...	T3

Source	URL	Tier
Anydesk to Quick Assist - possible overreaction due to breach news	https://www.reddit.com/r/sysadmin/comments/1arydts/anydesk_to_quick...	T3
Cross■tenant helpdesk impersonation to data exfiltration - Microsoft	https://www.microsoft.com/en-us/security/blog/2026/04/18/crosstenan...	T1
Microsoft Teams Social Engineering Delivers A0Backdoor Malware	https://hivepro.com/threat-advisory/microsoft-teams-social-engineer...	T3
Top 10 Remote Support Software for IT Teams in 2026 - Zoho Assist	https://www.zoho.com/assist/articles/top-remote-support-software-fo...	T3

Generated 2026-06-08 13:48 UTC by TJS Security Command Center