INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-05 08:18 UTC

RMM Tool Abuse Hits 80+ Organizations: Attackers Turn Trusted Software Into Phishing Infrastructure

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0270
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Unspecified legitimate RMM tools (two named in full article); enterprise environments with RMM deployments
Published	2026-05-04T16:56:34
Discovery Source	Rss

Executive Summary

Threat actors are exploiting legitimate remote monitoring and management (RMM) software to infiltrate enterprise environments, with confirmed impact across more than 80 organizations. Attackers deliver signed, trusted RMM binaries through phishing lures impersonating Zoom, Google Meet, and Microsoft Teams, giving them persistent, broad network access that blends into normal IT operations. Because the tools themselves are legitimate, standard allowlisting and signature-based defenses do not flag the activity, leaving organizations exposed to data theft, lateral movement, and prolonged undetected access.

Technical Analysis

Attackers are abusing at least two legitimate, signed RMM tools (named in the full Netskope report) to establish persistent remote access following phishing-based initial delivery. The attack chain maps to T1566/T1566.001/T1566.002 (phishing, spearphishing attachment/link), T1105 (ingress tool transfer), T1036/T1036.005 (masquerading, matching legitimate names), T1078 (valid accounts), and T1219 (remote access software). Because the RMM binaries are legitimately signed, endpoint detection relying on code signing or allowlisting is bypassed by design. CWE-494 (Download of Code Without Integrity Check) applies where the delivery mechanism lacks integrity verification. CWE-506 (Embedded Malicious Code) applicability is uncertain from available reporting, the binaries appear to be abused as-is rather than trojanized; this distinction should be confirmed against the full Netskope and Dark Reading articles before use in formal risk documentation. Qualitative severity rating (high) is set editorially based on scope and impact; CVSS vector scoring is not

confirmed from available source stubs and is not applicable to this campaign-type threat activity. No CVE identifier is associated with this campaign, this is an abuse-of-legitimate-tools pattern, not a software vulnerability. No patch exists to remediate the root cause; mitigations are detection and access-control focused. Primary sources: Netskope blog (direct campaign analysis), Huntress, Intel 471, and Immersive Labs (RMM misuse tradecraft).

Action Checklist

1. Containment Audit all RMM tools currently authorized and deployed across your environment. Identify any RMM binaries running outside approved change windows, on endpoints where IT did not initiate a session, or under user accounts that should not be running RMM software. Suspend unauthorized sessions immediately and isolate affected endpoints from the network pending investigation.
2. Detection Query endpoint telemetry and EDR logs for execution of RMM binaries (e.g., process creation events) initiated by user-context processes rather than system or IT-admin processes. Cross-reference against T1219 (remote access software) behavioral indicators in your SIEM. Review email gateway logs for phishing lures impersonating Zoom, Google Meet, or Microsoft Teams delivering executable payloads or links to RMM installers. Check network logs for outbound RMM relay traffic to cloud-hosted RMM infrastructure outside your approved vendor list.
3. Eradication Remove any unauthorized RMM tool installations identified during detection. Revoke sessions and rotate credentials for any accounts that interacted with unauthorized RMM processes. If trojanized binaries are found (rather than legitimate tools abused), treat as a full compromise, isolate, image, and rebuild affected endpoints. Confirm binary integrity against vendor-published hashes before re-approving any RMM tool.
4. Recovery Validate that no persistent access mechanisms (scheduled tasks, registry run keys, service installations) were established by the RMM tool during unauthorized sessions (MITRE T1053, T1547). Monitor for re-establishment of outbound RMM connections from previously affected endpoints for at least 30 days. Confirm that phishing lure delivery paths (email, collaboration platform messages) have been remediated and similar lures are blocked at the gateway.
5. Post-Incident This campaign exploits the gap between allowlisting legitimate tools and monitoring how those tools are used. Implement behavioral controls: restrict RMM execution to approved IT admin accounts and managed endpoints via application control policy, not just binary allowlisting. Establish a formal RMM inventory and require change-ticket correlation for all remote sessions. Review T1219 detection coverage in your SIEM against MITRE ATT&CK and close gaps identified by this incident.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership, legal counsel, and potentially CISA (per CISA reporting guidelines) if unauthorized RMM sessions are confirmed on endpoints with access to PII, PHI, or financial data (triggering breach notification obligations under HIPAA, GDPR, or state privacy laws), if lateral movement beyond the initial endpoint is detected, or if the team lacks the forensic capacity to image and analyze affected endpoints before evidence is lost.

Recovery Notes	Before returning any affected endpoint to production, validate that all RMM-related persistence mechanisms (scheduled tasks via Event ID 106, services via Event ID 7045, registry run keys) have been removed and confirmed clean by Autoruns scan. Maintain enhanced outbound network monitoring specifically for known RMM relay infrastructure (cloud-hosted relay domains for AnyDesk, ScreenConnect, Atera, and similar tools) on all previously affected endpoints for a minimum of 30 days, as threat actors in this campaign have demonstrated re-access capability through re-phishing the same users. Confirm with the RMM vendor that the attacker's tenant or license account has been disabled and obtain written confirmation as a record artifact.
Forensic Artifacts	RMM tool trace/session logs stored locally on affected endpoints (e.g., AnyDesk: %APPDATA%\AnyDesk\ad_svc.trace; ScreenConnect: %PROGRAMDATA%\ScreenConnect Client\logs\) — contain attacker session timestamps, relay server hostnames, and remote IP addresses used during unauthorized access. | Sysmon Event ID 1 (Process Creation) entries showing the full command line of the RMM installer binary, including any embedded session tokens, tenant IDs, or relay configuration parameters passed as arguments — these directly identify the attacker's RMM account. | Email gateway or M365 message trace logs capturing the phishing lure delivery: sender address, spoofed display name (Zoom/Google Meet/Microsoft Teams), attachment name or URL, and recipient list — establishes full blast radius of the phishing campaign. | Browser download history from affected user profiles (%LOCALAPPDATA%\Google\Chrome\User Data\Default\History or equivalent Edge/Firefox paths) containing the URL from which the RMM binary was downloaded — identifies the attacker's staging infrastructure. | Windows Security Event Log Event ID 4688 (Process Creation with command line logging enabled) and Sysmon Event ID 3 (Network Connection) correlated by PID to the RMM process — maps the full execution chain from phishing lure to RMM execution and captures all outbound relay connections made during unauthorized sessions.

Per-Action IR Details

Containment — Audit all RMM tools currently authorized and deployed across your environment. Identify any RMM binaries running outside approved change windows, on endpoints where IT did not initiate a session, or under user accounts that should not be running RMM software. Suspend unauthorized sessions immediately and isolate affected endpoints from the network pending investigation.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 — Containment Strategy: isolate affected systems to prevent attacker lateral movement while preserving evidence; choose containment strategy based on potential damage and need for evidence preservation.

Controls: NIST IR-4 (Incident Handling), NIST AC-2 (Account Management), NIST CM-8 (System Component Inventory), CIS 1.1 (Establish and Maintain Detailed Enterprise Asset Inventory), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Run the following PowerShell on all Windows endpoints (or distribute via GPO logon script): `Get-Process | Where-Object {$_.Name -match 'atera|screenconnect|anydesk|connectwise|splashtop|netsupport|zoho|datto|kaseya'} | Select-Object Name,Id,Path,StartTime,@{n='Owner';e={(Get-WmiObject Win32_Process -Filter "ProcessId=$($_.Id)").GetOwner().User}} | Export-Csv C:\IR\rmm_audit.csv`. Cross-reference output against your approved RMM vendor list and IT change tickets. Immediately terminate processes not matching approved tools: `Stop-Process -Id -Force`. For network isolation on Windows without EDR, use: `netsh advfirewall set allprofiles firewallpolicy blockinbound,blockoutbound` on suspect hosts.

Evidence: BEFORE isolating, capture: (1) Full process tree snapshot showing parent-child relationships — specifically look for RMM binary spawned by user-context processes (explorer.exe, outlook.exe, teams.exe, zoom.exe) rather than

SYSTEM or IT admin accounts, using `Get-WmiObject Win32_Process | Select ProcessId,ParentProcessId,Name,CommandLine,ExecutablePath | Export-Csv C:\IR\proctree.csv`; (2) Active network connections from the RMM process: `netstat -anob > C:\IR\netstat_$(hostname).txt`; (3) RMM binary file path, SHA-256 hash (`Get-FileHash -Algorithm SHA256`), and digital signature details (`Get-AuthenticodeSignature `) to distinguish legitimate signed binary from trojanized variant; (4) Windows Security Event Log entries for Event ID 4688 (Process Creation) and Event ID 4624/4625 (Logon Success/Failure) filtered to the RMM process name and the user account running it.

Detection — Query endpoint telemetry and EDR logs for execution of RMM binaries (e.g., process creation events) initiated by user-context processes rather than system or IT-admin processes. Cross-reference against T1219 (remote access software) behavioral indicators in your SIEM. Review email gateway logs for phishing lures impersonating Zoom, Google Meet, or Microsoft Teams delivering executable payloads or links to RMM installers. Check network logs for outbound RMM relay traffic to cloud-hosted RMM infrastructure outside your approved vendor list.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2 — Detection and Analysis: correlate indicators across multiple log sources; use attack vector knowledge (phishing lures impersonating Zoom/Teams/Meet) to scope detection queries and establish scope of compromise.

Controls: NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST IR-5 (Incident Monitoring), CIS 8.2 (Collect Audit Logs), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Deploy Sysmon with SwiftOnSecurity config (https://github.com/SwiftOnSecurity/sysmon-config) and enable Event ID 1 (Process Create) and Event ID 3 (Network Connection). Use this Sigma-compatible query logic targeting Sysmon Event ID 1: filter where `ParentImage` matches `*\outlook.exe`, `*\chrome.exe`, `*\msedge.exe`, `*\teams.exe`, `*\zoom.exe` AND `Image` matches known RMM binary names. For email phishing detection without a gateway: search Exchange/M365 message trace or on-prem mail logs for sender domains spoofing zoom.us, meet.google.com, or microsoft.com delivering `.exe`, `.msi`, or `.zip` attachments, or URLs containing RMM vendor download domains (e.g., `get.screenconnect.com`, `anydesk.com/download`). For network detection without SIEM: run Wireshark/tcpdump on egress firewall capturing outbound TCP 443 to cloud relay domains (e.g., `*.screenconnect.com`, `relay.atera.com`, `*.anydesk.com`) from endpoints where IT did not initiate a session.

Evidence: BEFORE concluding detection scope: (1) Export email gateway or M365 message trace logs filtered to the 72-hour window prior to first RMM execution, searching sender display names containing 'Zoom', 'Google Meet', or 'Microsoft Teams' with attachment types `.exe/.msi/.zip` or URL bodies matching RMM vendor download paths; (2) Sysmon Event ID 1 logs showing full command-line arguments of the RMM installer — installer command lines often include embedded session tokens or tenant IDs that identify the attacker's RMM account; (3) DNS query logs (Windows DNS debug log or Zeek `dns.log`) for resolution of attacker-controlled RMM relay infrastructure outside your approved vendor list; (4) Browser download history from affected user profiles (`%LOCALAPPDATA%\Google\Chrome\User Data\Default\History`, Edge equivalent) to confirm the phishing delivery URL and identify other endpoints that may have visited the same lure.

Eradication — Remove any unauthorized RMM tool installations identified during detection. Revoke sessions and rotate credentials for any accounts that interacted with unauthorized RMM processes. If trojanized binaries are found (rather than legitimate tools abused), treat as a full compromise — isolate, image, and rebuild affected endpoints. Confirm binary integrity against vendor-published hashes before re-approving any RMM tool.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication: eliminate components of the incident (malicious code, unauthorized accounts/access) and mitigate vulnerabilities that were exploited; confirm eradication before recovery.

Controls: NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AC-2 (Account Management), CIS 2.3 (Address Unauthorized Software), CIS 5.3 (Disable Dormant Accounts)

Compensating: For uninstallation: run `wmic product where "name like '%AnyDesk%'" call uninstall` (substitute RMM product name) and confirm removal with `Get-ItemProperty HKLM:\Software\Microsoft\Windows\CurrentVersion\Uninstall\* | Where DisplayName -match "`. For binary integrity verification without enterprise tooling: download vendor-published SHA-256 hashes from the official vendor advisory page and compare using `Get-FileHash -Algorithm SHA256`. For credential rotation on a 2-person team: prioritize accounts where Event ID 4624 (Logon) was recorded from the RMM process; use `net user /domain` to enumerate group memberships before rotating, then reset via `Set-ADAccountPassword`. For imaging prior to rebuild: use free tool `FTK Imager Lite` (portable, no install required) to capture a forensic image before wiping.

Evidence: BEFORE removing artifacts: (1) Capture RMM installation directory contents and file hashes — common paths include `%PROGRAMFILES%\\`, `%APPDATA%\\`, and `%LOCALAPPDATA%\Temp\` (phishing-delivered installers frequently stage here); (2) Export HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall and HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run for RMM-related entries; (3) Record all Windows Security Event ID 4648 (Explicit Credential Logon) and Event ID 4672 (Special Privileges Assigned) events associated with accounts that had active RMM sessions during the unauthorized window; (4) Capture the RMM session/connection log files stored locally by the tool — AnyDesk logs at `%APPDATA%\AnyDesk\ad_svc.trace`, ConnectWise ScreenConnect at `%PROGRAMDATA%\ScreenConnect Client\logs\` — these contain attacker session timestamps and relay server addresses.

Recovery — Validate that no persistent access mechanisms (scheduled tasks, registry run keys, service installations) were established by the RMM tool during unauthorized sessions (MITRE T1053, T1547). Monitor for re-establishment of outbound RMM connections from previously affected endpoints for at least 30 days. Confirm that phishing lure delivery paths (email, collaboration platform messages) have been remediated and similar lures are blocked at the gateway.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery: restore systems to normal operations, confirm no residual attacker access, and implement additional monitoring to detect recurrence before closing the incident.

Controls: NIST IR-4 (Incident Handling), NIST SI-4 (System Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CM-8 (System Component Inventory), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: Persistence sweep without EDR: run `schtasks /query /fo LIST /v > C:\IR\scheduled_tasks.txt` and review for tasks created during the unauthorized RMM session window; check `HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, `HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run`, and `HKLM\SYSTEM\CurrentControlSet\Services` using `reg export` for offline review. For service-based persistence: `Get-WmiObject Win32_Service | Where-Object {$_.PathName -match "} | Select Name,State,PathName`. For 30-day outbound monitoring without SIEM: configure a firewall deny rule for known attacker RMM relay domains/IPs with logging enabled, and set a daily cron/scheduled task to parse firewall logs for hits: `Select-String -Path C:\Windows\System32\LogFiles\Firewall\pfirewall.log -Pattern "`. Deploy free YARA rule matching RMM binary characteristics to scan new files in `%TEMP%` and `%APPDATA%` weekly.

Evidence: BEFORE declaring recovery complete: (1) Run Autoruns (Sysinternals, portable) on all previously affected endpoints and export full results to CSV — specifically review the Scheduled Tasks, Services, and Logon tabs for entries with timestamps correlating to the unauthorized RMM session window; (2) Query Windows System Event Log Event ID 7045 (New Service Installed) and Task Scheduler Event Log (Microsoft-Windows-TaskScheduler/Operational) Event ID 106 (Task Registered) for the incident timeframe; (3) Confirm email gateway or M365 rules are in place blocking delivery of executables from domains spoofing zoom.us, google.com (meet subdomains), and microsoft.com — export the current block rule list as a configuration artifact; (4) Verify that the attacker's RMM tenant/account has been reported to the RMM vendor for deactivation and document the vendor ticket number.

Post-Incident — This campaign exploits the gap between allowlisting legitimate tools and monitoring how those tools are used. Implement behavioral controls: restrict RMM execution to approved IT admin accounts and managed endpoints via application control policy, not just binary allowlisting. Establish a formal RMM

inventory and require change-ticket correlation for all remote sessions. Review T1219 detection coverage in your SIEM against MITRE ATT&CK and close gaps identified by this incident.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §4 — Post-Incident Activity: conduct lessons-learned review, update detection and response capabilities, and share intelligence to prevent recurrence; update IR plan with controls that address the specific gap exploited.

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST SI-4 (System Monitoring), NIST AU-2 (Event Logging), NIST CM-8 (System Component Inventory), CIS 2.1 (Establish and Maintain a Software Inventory), CIS 2.2 (Ensure Authorized Software is Currently Supported), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For behavioral application control without enterprise tooling: use Windows AppLocker (available on Windows 10/11 Pro and Enterprise) to create a rule set that allows RMM binaries ONLY when executed by accounts in the IT Admins security group — configure via `secpol.msc` > Application Control Policies > AppLocker > Executable Rules, set condition to publisher (leveraging the signed binary's certificate) AND user group restriction. For change-ticket correlation on a small team: create a shared spreadsheet (or git-tracked YAML file) as the RMM session registry — require IT staff to log session start/end, endpoint, and ticket number before initiating any RMM session, and configure your RMM tool's audit log export to run nightly for comparison. Implement the MITRE ATT&CK T1219 Sigma rule (available at https://github.com/SigmaHQ/sigma — search `remote_access_software`) against Sysmon logs to close the detection gap identified in this incident.

Evidence: For the lessons-learned record: (1) Compile the full timeline from phishing email delivery timestamp through RMM binary execution, unauthorized session activity, and detection — sourced from email gateway logs, Sysmon Event ID 1, and RMM tool audit logs; (2) Document the specific RMM vendor names and tenant/session IDs used by the attacker (extracted from RMM trace logs during eradication) to support threat intelligence sharing with sector ISACs or CISA; (3) Record the MITRE ATT&CK technique gaps identified: T1219 (Remote Access Software), T1566 (Phishing — specifically T1566.002 Spearphishing Link if delivered via URL), and T1053/T1547 persistence techniques — document which detections fired and which did not, as the primary output for SIEM rule improvement.

Detection Guidance

Focus detection on behavioral anomalies, not binary signatures, the RMM tools are legitimately signed and will not trigger signature-based alerts. Key detection signals: (1) RMM process execution spawned by a user-context process (e.g., browser, email client, Teams/Zoom installer) rather than an IT admin account or system process, flag parent-child process chains involving known RMM binary names; (2) RMM binary executions on endpoints with no corresponding IT change ticket or approved remote session in your ITSM system; (3) outbound network connections from RMM processes to cloud relay infrastructure for RMM vendors not on your approved vendor list; (4) email gateway alerts on messages impersonating Zoom, Google Meet, or Microsoft Teams that contain executable attachments or links to executable downloads. MITRE technique coverage to validate: T1219 (remote access software), T1566.001/T1566.002 (phishing), T1036.005 (masquerading). Intel 471's RMM threat hunting guide (source listed) provides structured hunting hypotheses. Huntress's 'Series of Unfortunate RMM Events' post includes behavioral indicators specific to RMM abuse patterns. Note: specific IOCs (hashes, domains, IPs) are not available from the source stubs provided, consult the full Netskope blog post for campaign-specific indicators.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`Not available from source stubs`	Campaign-specific IOCs (hashes, C2 domains, delivery URLs) are referenced in the full Netskope blog post but are not present in the source data provided. Consult https://www.netskope.com/blog/attackers-weaponize-signed-rmm-tools-via-zoom-meet-teams-lures directly for current indicators.	LOW

Framework Mappings

MITRE-ATTACK

- **T1566** — Phishing
- **T1566.002** — Spearphishing Link
- **T1105** — Ingress Tool Transfer
- **T1036** — Masquerading
- **T1078** — Valid Accounts
- **T1566.001** — Spearphishing Attachment
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1219** — Remote Access Tools

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
- **SI-7** — Software, Firmware, and Information Integrity
- **CM-3** — Configuration Change Control

OWASP-TOP10-2021

- **A08:2021** — Software and Data Integrity Failures

CIS-V8

- **2.5** — Allowlist Authorized Software
- **2.6** — Allowlist Authorized Libraries

- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

- **164.308(a)(5)(i)** — Security Awareness and Training

ISO-27001-2022

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

NIST-CSF-2

- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1566	Phishing	Initial-Access
T1566.002	Spearphishing Link	Initial-Access
T1105	Ingress Tool Transfer	Command-And-Control
T1036	Masquerading	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1566.001	Spearphishing Attachment	Initial-Access
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1219	Remote Access Tools	Command-And-Control

Sources

Source	URL	Tier
Security News	https://www.darkreading.com/cyberattacks-data-breaches/rmm-tools-st...	T3
Understanding and threat hunting for RMM software misuse | Intel 471	https://www.intel471.com/blog/understanding-and-threat-hunting-for-...	T3
RMM Tools Under Attack: Exploring More Effective Detections	https://www.immersivelabs.com/resources/c7-blog/rmm-tools-under-att...	T3
A Series of Unfortunate (RMM) Events - Huntress	https://www.huntress.com/blog/series-of-unfortunate-rmm-events	T3

Source	URL	Tier
Attackers Weaponize RMM Tools via Zoom, Meet, & Teams Lures	https://www.netskope.com/blog/attackers-weaponize-signed-rmm-tools-...	T3

Generated 2026-05-05 08:18 UTC by TJS Security Command Center