INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-20 18:51 UTC

# Microsoft Teams Helpdesk Impersonation: Nine-Stage Social Engineering Chain Abuses Quick Assist and Rclone for Enterprise Compromise

**THREAT CAMPAIGN** | **HIGH** | CVSS 7.5

| | |
|---|---|
| **SCC Item ID** | SCC-CAM-2026-0189 |
| **Type** | Threat Campaign |
| **Severity** | HIGH |
| **CVSS Base Score** | 7.5 |
| **Affected Products** | Microsoft Teams (External Chat), Quick Assist, Windows Remote Management (WinRM), Rclone, Autodesk, Adobe Acrobat/Reader, Windows Error Reporting |
| **Published** | 2026-04-20T11:11:24 |
| **Discovery Source** | Rss |

## Executive Summary

Threat actors are impersonating IT helpdesk staff over Microsoft Teams external chat, then using Microsoft's own Quick Assist remote access tool to take control of employee workstations. Once inside, attackers install hidden backdoors disguised as legitimate software (Autodesk, Adobe Acrobat), exfiltrate data using Rclone, and cover their tracks using built-in Windows tools. Any organization using Microsoft Teams with external communications enabled is exposed, and successful compromise can result in full network access, data theft, and ransomware deployment.

## Technical Analysis

This campaign, documented by Microsoft in two security blog posts (March 2026), chains nine stages to achieve enterprise compromise without traditional exploit code. Attack vector: Microsoft Teams external chat (T1566.004) used to initiate contact and establish false helpdesk identity. The attacker convinces the target to launch Quick Assist (T1219), granting interactive remote session access. Post-access, the attacker deploys LOLBins including WinRM (T1021.006) and executes commands via cmd.exe and PowerShell (T1059.003, T1059.001). Persistence is established via registry run keys (T1547.001) and signed malware masquerading as Autodesk or Adobe Acrobat/Reader installers (T1036.005, T1574.002). Windows Error Reporting is abused for defense evasion (T1562, T1562.001). Final-stage exfiltration uses Rclone to cloud storage endpoints (T1567, T1567.002). Relevant CWEs: CWE-427 (uncontrolled search path), CWE-1021 (improper frame restrictions),

CWE-693 (protection mechanism failure), CWE-426 (untrusted search path). No CVE assigned. Structural overlap noted with Black Basta Teams abuse campaigns; attribution remains unconfirmed. Microsoft disclosed technical detail across two security blog posts dated 2026-03-03 and 2026-03-16. No patch resolves this campaign; it abuses legitimate, intended functionality.

## Action Checklist

1. Containment, Restrict or disable Microsoft Teams external access immediately for user populations that do not require it. In Teams Admin Center, navigate to External Access settings and block or allowlist specific external domains rather than permitting all external communication. Disable Quick Assist enterprise-wide via Group Policy (Computer Configuration > Administrative Templates > System > Remove Quick Assist) or block the executable (quickassist.exe) via application control policy if Quick Assist is not operationally required. Note: Quick Assist may be re-enabled by Windows Update; verify the Group Policy setting persists after patches and monitor for unexpected re-enablement.
2. Detection, Query Unified Audit Logs and Microsoft Teams audit logs for external-initiated chat sessions, particularly from free or consumer Microsoft accounts contacting internal users. Hunt for quickassist.exe parent-child process chains spawning cmd.exe, powershell.exe, or msiexec.exe. Search EDR telemetry for Rclone execution, especially rclone.exe with 'copy' or 'sync' arguments to cloud storage endpoints. Review Windows Event ID 4688 (process creation) for WinRM activity (wsmprovhost.exe) initiated from unexpected sources. Flag signed executables claiming to be Autodesk or Adobe products installed outside standard software deployment paths.
3. Eradication, There is no patch; the attack abuses legitimate Microsoft functionality. Block Rclone (hash-based or filename-based) via endpoint protection policy. Remove any unauthorized RMM tools, scheduled tasks, or registry run keys added outside approved deployment channels. Revoke any Quick Assist sessions in progress and audit remote session logs. Re-image systems where unauthorized remote access is confirmed.
4. Recovery, After removing unauthorized access and tooling, validate registry run key baselines (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and equivalent user-level keys) against known-good snapshots. Confirm no unauthorized accounts were created (Event ID 4720) or elevated (Event ID 4672, 4728). Monitor cloud storage audit logs for continued Rclone-originated uploads. Restore affected endpoints from clean images where forensic integrity is uncertain.
5. Post-Incident, Conduct user awareness training specific to Teams-based helpdesk impersonation: legitimate internal IT teams do not initiate contact via Teams external chat. Implement a verified IT support contact process with a known internal Teams channel or ticketing system. Enforce application allowlisting to prevent unauthorized installer execution. Review and tighten Teams external access policies as a standing control, not a one-time response.

## IR / Forensic Enrichment

| | |
|---|---|
| **Triage Priority** | IMMEDIATE |

| | |
|---|---|
| **Escalation Criteria** | Escalate to executive leadership, legal counsel, and potentially law enforcement if Rclone exfiltration is confirmed to cloud storage endpoints (indicating data theft of PII, PHI, or IP), if unauthorized accounts were created in Active Directory or Azure AD, or if compromise scope extends beyond a single endpoint — any of these conditions may trigger breach notification obligations under GDPR, HIPAA, or state-level data protection laws. |
| **Recovery Notes** | After re-imaging confirmed compromised endpoints, maintain elevated monitoring of Teams external communication logs and WinRM activity for a minimum of 30 days, as this campaign's use of legitimate Microsoft tooling (Quick Assist, WinRM) means re-compromise attempts may not trigger standard malware alerts. Validate that all Rclone-associated OAuth tokens or cloud storage authorizations have been revoked in your identity provider, and cross-reference Azure AD audit logs for any persistent app permissions granted during the compromise window. Treat any endpoint where Quick Assist was actively used by an external party as fully compromised and re-image rather than attempting remediation in place, given the attacker had interactive desktop control and the ability to stage additional persistence mechanisms beyond what forensics may recover. |
| **Forensic Artifacts** | Microsoft Purview Unified Audit Log (UAL) — RecordType=MicrosoftTeams operations filtered for external sender domains (outlook.com, hotmail.com, live.com) contacting internal users: this is the primary artifact establishing the social engineering entry vector and attacker-controlled Microsoft account identifiers \| Windows Event Log: Applications and Services Logs > Microsoft > Windows > RemoteAssistance-Gui > Operational — Event IDs 101/102 recording Quick Assist session initiation and acceptance, including timestamps and session handles that correlate to the attacker's interactive access window \| Prefetch files at %SystemRoot%\Prefetch\RCLONE.EXE-*.pf and QUICKASSIST.EXE-*.pf — establish first-execution timestamps for both tools independently of potentially tampered Event Logs, and RCLONE.EXE prefetch will contain the last 8 directory paths accessed, potentially revealing staged exfiltration source folders \| File system artifacts in %AppData%\Local\Temp, %ProgramData%, and non-standard install paths for MSI or EXE files with spoofed Autodesk or Adobe Acrobat digital signatures — these dropped backdoors are the persistent access mechanism and will have creation timestamps aligning to the Quick Assist session window \| Windows Registry hive NTUSER.DAT and HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run — persistence keys written by the backdoor installers during the Quick Assist session; also check HKLM\SYSTEM\CurrentControlSet\Services for any new services registered by the attacker-deployed tooling disguised as Autodesk or Adobe components |

### Per-Action IR Details

**Containment — Restrict or disable Microsoft Teams external access immediately for user populations that do not require it. In Teams Admin Center, navigate to External Access settings and block or allowlist specific external domains rather than permitting all external communication. Disable Quick Assist enterprise-wide via Group Policy (Computer Configuration > Administrative Templates > System > Remove Quick Assist) or block the executable (quickassist.exe) via application control policy if Quick Assist is not operationally required.**

**NIST Phase:** Containment

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

**Controls:** NIST IR-4 (Incident Handling), NIST CM-7 (Least Functionality), NIST SC-7 (Boundary Protection), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices)

**Compensating:** Without enterprise MDM, push a GPO immediately: Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies — add a DENY rule for %SystemRoot%\System32\quickassist.exe and %ProgramFiles%\WindowsApps\MicrosoftCorporationII.QuickAssist*\QuickAssist.exe. For Teams external access without a Teams Admin Center license tier that exposes those controls, use the PowerShell module:

Connect-MicrosoftTeams; Set-CsTenantFederationConfiguration -AllowFederatedUsers $false. One analyst executes GPO, one validates enforcement via rsop.msc on a sample endpoint within 30 minutes.

**Evidence:** Before restricting Teams external access, export the full Teams External Access configuration audit trail via Microsoft Purview Unified Audit Log (UAL) — search for operation 'TeamsSessionStarted' and 'MeetingDetail' filtered to ExternalParticipant fields. Capture the list of all active Quick Assist session handles from the Windows Event Log: Applications and Services Logs > Microsoft > Windows > RemoteAssistance-Gui > Operational, Event ID 101 (session initiated) and 102 (session accepted). Screenshot or export Teams Admin Center External Access configuration before any policy changes to document pre-incident state.

**Detection — Query Unified Audit Logs and Microsoft Teams audit logs for external-initiated chat sessions, particularly from free or consumer Microsoft accounts contacting internal users. Hunt for quickassist.exe parent-child process chains spawning cmd.exe, powershell.exe, or msiexec.exe. Search EDR telemetry for Rclone execution, especially rclone.exe with 'copy' or 'sync' arguments to cloud storage endpoints. Review Windows Event ID 4688 (process creation) for WinRM activity (wsmprovhost.exe) initiated from unexpected sources. Flag signed executables claiming to be Autodesk or Adobe products installed outside standard software deployment paths.**

**NIST Phase:** Detection Analysis

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

**Controls:** NIST IR-5 (Incident Monitoring), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST AU-12 (Audit Record Generation), NIST SI-4 (System Monitoring), CIS 8.2 (Collect Audit Logs)

**Compensating:** Without EDR, deploy Sysmon with SwiftOnSecurity config (github.com/SwiftOnSecurity/sysmon-config) and hunt using these specific queries — (1) Sysmon Event ID 1 (Process Create): ParentImage contains 'quickassist.exe' AND Image contains any of 'cmd.exe','powershell.exe','msiexec.exe'; (2) Sysmon Event ID 3 (Network Connect): Image contains 'rclone.exe' AND DestinationPort in (443,80) to non-corporate IPs; (3) Windows Security Event ID 4688 with CommandLine containing 'wsmprovhost' or 'winrm'. For Teams UAL without a SIEM, run: Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date) -RecordType MicrosoftTeams -Operations 'MessageCreatedHasLink,MessageSent' | Where-Object {$_.AuditData -like '*external*'} | Export-Csv teams_external_audit.csv. Use Sigma rule 'proc_creation_win_rclone_exec.yml' (SigmaHQ) converted to PowerShell for Event Log querying.

**Evidence:** Capture before analysis: (1) Microsoft Purview UAL export for RecordType=MicrosoftTeams covering the suspected compromise window, filtering on ExternalAccess=true and sender domains ending in outlook.com, hotmail.com, or gmail.com (consumer Microsoft accounts used by threat actor); (2) Sysmon or Security Event ID 4688 logs from all endpoints showing quickassist.exe execution and its child process tree; (3) Prefetch files (%SystemRoot%\Prefetch\RCLONE.EXE-*.pf and QUICKASSIST.EXE-*.pf) to establish first-execution timestamps; (4) Windows Registry key HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\AppCompatFlags\Compatibility Assistant\Store for evidence of rclone.exe execution even if logs were cleared; (5) WinRM operational log at Applications and Services Logs > Microsoft > Windows > WinRM > Operational for remote session establishment events.

**Eradication — There is no patch; the attack abuses legitimate Microsoft functionality. Block Rclone (hash-based or filename-based) via endpoint protection policy. Remove any unauthorized RMM tools, scheduled tasks, or registry run keys added outside approved deployment channels. Revoke any Quick Assist sessions in progress and audit remote session logs. Re-image systems where unauthorized remote access is confirmed.**

**NIST Phase:** Eradication

**Reference:** NIST 800-61r3 §3.4 — Eradication and Recovery

**Controls:** NIST IR-4 (Incident Handling), NIST SI-2 (Flaw Remediation), NIST SI-3 (Malicious Code Protection), NIST CM-7 (Least Functionality), CIS 2.3 (Address Unauthorized Software), CIS 7.2 (Establish and Maintain a Remediation Process)

**Compensating:** Without enterprise endpoint protection, use these manual eradication steps: (1) Block Rclone by SHA-256 hash using Windows Defender via PowerShell: Add-MpPreference -ExclusionPath is NOT what you want — instead use: New-CIPolicy then Add-SignerRule, or simpler: use WDAC in audit mode first with a policy that denies rclone.exe by file hash obtained from VirusTotal or your IR image; (2) Query all scheduled tasks across affected hosts: Get-ScheduledTask | Where-Object {$_.TaskPath -notlike '\Microsoft*'} | Select TaskName,TaskPath,@{N='Action';E={$_.Actions.Execute}} | Export-Csv schtasks_audit.csv — review for entries pointing to temp directories, AppData, or ProgramData; (3) Query unauthorized registry run keys: Get-ItemProperty 'HKLM:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run','HKCU:\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and diff against your baseline; (4) Terminate active Quick Assist sessions: Get-Process quickassist | Stop-Process -Force on affected endpoints.

**Evidence:** Before re-imaging, collect full forensic triage package: (1) Memory image using WinPmem (free) to capture any in-memory backdoor artifacts from the Autodesk- or Adobe-disguised malware dropped via Quick Assist; (2) Full copy of %AppData%\Local\Temp, %ProgramData%, and any non-standard install directories where attackers dropped disguised installers — these will contain the malicious MSI or EXE files with spoofed Autodesk/Adobe digital signatures; (3) Registry hive export (SYSTEM, SOFTWARE, NTUSER.DAT) from affected endpoints to preserve Run key persistence mechanisms; (4) Collect all scheduled task XML definitions from C:\Windows\System32\Tasks\ before clearing; (5) Export Windows Event Logs (Security, System, Application, Sysmon) as .evtx files before re-image destroys them.

**Recovery — After removing unauthorized access and tooling, validate registry run key baselines (HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and equivalent user-level keys) against known-good snapshots. Confirm no unauthorized accounts were created (Event ID 4720) or elevated (Event ID 4672, 4728). Monitor cloud storage audit logs for continued Rclone-originated uploads. Restore affected endpoints from clean images where forensic integrity is uncertain.**

**NIST Phase:** Recovery

**Reference:** NIST 800-61r3 §3.5 — Recovery

**Controls:** NIST IR-4 (Incident Handling), NIST CP-10 (System Recovery and Reconstitution), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 5.3 (Disable Dormant Accounts)

**Compensating:** Without SIEM for continuous monitoring, implement these manual recovery validation steps: (1) Account audit: Get-WinEvent -FilterHashtable @{LogName='Security';Id=4720,4672,4728} -MaxEvents 1000 | Select TimeCreated,Message | Export-Csv account_changes.csv — review for any accounts created or elevated during the compromise window; (2) Registry baseline diff: if no prior snapshot exists, compare against CIS Benchmarks baseline for Windows run keys and remove any entries pointing to non-standard paths (AppData, Temp, ProgramData); (3) For cloud exfiltration monitoring without a CASB, enable Microsoft Defender for Cloud Apps 30-day trial or query Azure AD sign-in logs for OAuth app authorizations granted to Rclone or unknown cloud storage apps: Get-MgAuditLogSignIn -Filter "appDisplayName eq 'rclone'" ; (4) Re-image validation: after restore, run 'sfc /scannow' and compare installed software inventory against pre-incident baseline via: Get-WmiObject Win32_Product | Select Name,Version | Sort Name.

**Evidence:** Before declaring recovery complete, verify: (1) Windows Security Event ID 4720 (account created), 4722 (account enabled), 4728 (member added to global security group), and 4672 (special privileges assigned) for the entire compromise window — attackers in this campaign have created backdoor local accounts for persistence; (2) Cloud storage provider audit logs (OneDrive, SharePoint, or any CASB-monitored SaaS) for Rclone user-agent strings or OAuth tokens issued to unknown applications; (3) WinRM audit logs (Applications and Services Logs > Microsoft > Windows > WinRM > Operational) confirming no active remote sessions persist post-eradication; (4) Autoruns output (Sysinternals Autoruns run as SYSTEM, exported to CSV) from recovered endpoints to confirm no persistence mechanisms survive the cleanup.

**Post-Incident — Conduct user awareness training specific to Teams-based helpdesk impersonation: legitimate internal IT teams do not initiate contact via Teams external chat. Implement a verified IT support contact process with a known internal Teams channel or ticketing system. Enforce application allowlisting to prevent unauthorized installer execution. Review and tighten Teams external access policies as a standing**

**control, not a one-time response.**

**NIST Phase:** Post Incident

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

**Controls:** NIST IR-4 (Incident Handling), NIST IR-2 (Incident Response Training), NIST IR-8 (Incident Response Plan), NIST AT-2 (Literacy Training and Awareness), NIST CM-7 (Least Functionality), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 4.6 (Securely Manage Enterprise Assets and Software)

**Compensating:** Without a dedicated security awareness platform, create a one-page Teams-specific phishing recognition guide covering: (1) how to identify external-badge indicators on Teams messages (the 'External' tag displayed on contacts outside your tenant); (2) a simulated helpdesk impersonation tabletop exercise using a free consumer Microsoft account to demonstrate how convincingly attackers can spoof IT staff display names; (3) publish a pinned message in all-staff Teams channels with a screenshot showing what a legitimate internal IT contact looks like vs. an external impersonator; (4) for application allowlisting without a commercial tool, deploy Windows Defender Application Control (WDAC) using the Microsoft-recommended block rules policy (free, built into Windows 10/11 Enterprise) — start in audit mode, review Event ID 3076/3077 in Applications and Services Logs > Microsoft > Windows > CodeIntegrity > Operational, then enforce after 2-week baseline.

**Evidence:** For the post-incident lessons learned report (NIST 800-61r3 §4.1), preserve: (1) Complete Teams external chat history for all identified victim users, exported via Microsoft Purview Content Search filtered to the compromise timeframe, as the primary evidence of social engineering script and impersonation TTPs; (2) The full timeline of Quick Assist session IDs from RemoteAssistance-Gui Operational logs mapped to Active Directory user accounts to document which employees were targeted vs. compromised; (3) Rclone command-line arguments captured from process creation logs (Sysmon Event ID 1 or Security Event ID 4688) documenting destination cloud storage endpoints — this identifies what data was exfiltrated and to which attacker-controlled storage; (4) Any dropped installer files with spoofed Autodesk or Adobe signatures recovered from %AppData% or %Temp% for malware analysis and hash-based IOC development.

## Detection Guidance

Primary detection surface is process telemetry and Teams audit logs. Key behavioral indicators: (1) quickassist.exe spawning cmd.exe, powershell.exe, or msiexec.exe, flag immediately; (2) wsmprovhost.exe (WinRM provider host) executing without a known administrative workflow; (3) rclone.exe present on endpoints outside approved tooling, any execution should trigger alert; (4) signed executables with Autodesk or Adobe metadata installed to user-writable directories (AppData, Temp) rather than Program Files; (5) Windows Error Reporting (wermgr.exe, werfault.exe) spawning unexpected child processes. In Microsoft Teams audit logs, filter for external chat messages directed at internal users from non-corporate domains, particularly accounts on microsoft.com consumer tenants. SIEM query suggestion (generic SPL pattern): index=endpoint (process_name="quickassist.exe" AND (child_process="cmd.exe" OR child_process="powershell.exe")) OR (process_name="rclone.exe"). MITRE coverage gaps to address: T1219 (remote access tools), T1036.005 (signed binary masquerading), T1567.002 (exfiltration to cloud storage), validate existing detections against these technique IDs in your SIEM and EDR.

## Indicators of Compromise

| Type | Value | Context | Confidence |
|---|---|---|---|
| URL | `rclone cloud storage sync endpoints (generic — specific destination URLs not disclosed in source material)` | Rclone used for final-stage data exfiltration; specific cloud provider endpoints not confirmed in available sources | LOW |
| HASH | `Not available — specific file hashes for masquerading installers not disclosed in publicly available source material` | Signed malware impersonating Autodesk and Adobe Acrobat/Reader installers; hashes not released in March 2026 Microsoft blog posts | LOW |

## Framework Mappings

### MITRE-ATTACK

- **T1219** — Remote Access Tools
- **T1574.002** — DLL Side-Loading
- **T1547.001** — Registry Run Keys / Startup Folder
- **T1566.004** — Spearphishing Voice
- **T1059.003** — Windows Command Shell
- **T1021.006** — Windows Remote Management
- **T1567** — Exfiltration Over Web Service
- **T1566** — Phishing
- **T1059.001** — PowerShell
- **T1036** — Masquerading
- **T1083** — File and Directory Discovery
- **T1598** — Phishing for Information
- **T1078** — Valid Accounts
- **T1105** — Ingress Tool Transfer
- **T1562** — Impair Defenses
- **T1018** — Remote System Discovery
- **T1562.001** — Disable or Modify Tools
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1204** — User Execution
- **T1534** — Internal Spearphishing
- **T1567.002** — Exfiltration to Cloud Storage
- **T1204.002** — Malicious File

### NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection

- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-8** — Spam Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **AU-9** — Protection of Audit Information
- **CM-6** — Configuration Settings

**CIS-V8**

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

**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

**NIST-CSF-2**

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

## MITRE ATT&CK Mapping

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1219 | Remote Access Tools | Command-And-Control |
| T1574.002 | DLL Side-Loading | Persistence |
| T1547.001 | Registry Run Keys / Startup Folder | Persistence |
| T1566.004 | Spearphishing Voice | Initial-Access |
| T1059.003 | Windows Command Shell | Execution |
| T1021.006 | Windows Remote Management | Lateral-Movement |
| T1567 | Exfiltration Over Web Service | Exfiltration |

| Technique ID | Technique Name | Tactic |
|---|---|---|
| T1566 | Phishing | Initial-Access |
| T1059.001 | PowerShell | Execution |
| T1036 | Masquerading | Defense-Evasion |
| T1083 | File and Directory Discovery | Discovery |
| T1598 | Phishing for Information | Reconnaissance |
| T1078 | Valid Accounts | Defense-Evasion |
| T1105 | Ingress Tool Transfer | Command-And-Control |
| T1562 | Impair Defenses | Defense-Evasion |
| T1018 | Remote System Discovery | Discovery |
| T1562.001 | Disable or Modify Tools | Defense-Evasion |
| T1036.005 | Match Legitimate Resource Name or Location | Defense-Evasion |
| T1204 | User Execution | Execution |
| T1534 | Internal Spearphishing | Lateral-Movement |
| T1567.002 | Exfiltration to Cloud Storage | Exfiltration |
| T1204.002 | Malicious File | Execution |

## Sources

| Source | URL | Tier |
|---|---|---|
| **Security News** | https://www.bleepingcomputer.com/news/security/microsoft-teams-incr... | T3 |
| **Signed malware impersonating workplace apps deploys RMM ...** | https://www.microsoft.com/en-us/security/blog/2026/03/03/signed-mal... | T1 |
| **Help on the line: How a Microsoft Teams support call led to ...** | https://www.microsoft.com/en-us/security/blog/2026/03/16/help-on-th... | T1 |
| **20 minutes ago, it appeared that someone had illegal remote access.** | https://learn.microsoft.com/en-us/answers/questions/5822714/20-minu... | T1 |

| Source | URL | Tier |
|---|---|---|
| **Hackers Abuse Microsoft Teams for Remote Access via A0Backdoor ...** | https://www.linkedin.com/posts/cybersecurity-news_cybersecuritynews... | T3 |



Generated 2026-04-20 18:51 UTC by TJS Security Command Center