INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-06 18:52 UTC

MuddyWater (MOIS) Uses Chaos Ransomware as Espionage Cover via Microsoft Teams Social Engineering

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0281
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Microsoft Teams, Microsoft Quick Assist, Microsoft WebView2 (spoofed), AnyDesk, DWAgent, RDP
Published	2026-05-06T09:02:52
Discovery Source	Rss

Executive Summary

Iranian state-sponsored group MuddyWater, operating under Iran's Ministry of Intelligence and Security, conducted a targeted espionage campaign using Microsoft Teams to impersonate IT helpdesk staff and trick employees into granting remote access. Once inside, operators stole credentials, moved laterally across networks, and deployed Chaos ransomware as a cover story to disguise the true objective: intelligence gathering and espionage collection. Organizations using Microsoft Teams with external access enabled, particularly those in sectors of interest to Iranian intelligence, face direct risk of credential theft, data exfiltration, and prolonged undetected intrusion.

Technical Analysis

MuddyWater (MITRE G0069, attributed to MOIS) executed a cross-tenant Microsoft Teams social engineering campaign targeting enterprise environments. Initial access was achieved via Teams messages sent from attacker-controlled external tenants, with operators impersonating IT helpdesk personnel (T1566.004 spear-phishing via service; T1036, T1036.005, masquerading). Targets were directed to grant remote control via Microsoft Quick Assist, AnyDesk, and DWAgent (T1219, remote access tools). Post-access activity included credential harvesting (T1556, T1078, valid accounts; CWE-287, improper authentication; CWE-522, insufficiently protected credentials), lateral movement via RDP (T1021.001), data collection and archiving (T1560), and exfiltration over C2 channels (T1041, T1071.001). Operators deployed a Chaos ransomware payload (T1486) as a deception layer to simulate financially motivated cybercrime rather than espionage

(T1497, virtualization/sandbox evasion; CWE-693, protection mechanism failure). A spoofed Microsoft WebView2 component indicates potential browser-in-the-browser or in-session credential harvesting (CWE-1021, UI redress). Infrastructure overlap and code-signing certificates previously linked to MuddyWater tooling support attribution at moderate confidence per Rapid7. No CVE identifiers are associated with this campaign; exploitation relied on social engineering and legitimate remote access tooling, not unpatched software vulnerabilities. Rapid7 and Microsoft have both published on this campaign pattern; Microsoft's primary advisory is dated 2026-04-18.

Action Checklist

1. Step 1: Containment. Audit Microsoft Teams external access settings immediately. Restrict or disable cross-tenant external messaging for non-approved domains via the Microsoft Teams Admin Center under 'External Access' policies. Block AnyDesk and DWAgent executables at the endpoint and network perimeter if not business-required. Block Quick Assist execution (msra.exe) via AppLocker, Intune device restrictions, or EDR policy for non-IT users and non-support scenarios.
2. Step 2: Detection. Review Microsoft Teams audit logs (via Microsoft Purview / Unified Audit Log) for external tenant message threads, especially those referencing IT support, helpdesk, or urgent access requests. Search endpoint logs for Quick Assist (msra.exe, quickassist.exe), AnyDesk (AnyDesk.exe), and DWAgent process execution events. Hunt for RDP lateral movement (Event ID 4624 with LogonType 10, Event ID 131 in TerminalServices-RemoteConnectionManager). Check for Chaos ransomware indicators: file extension changes (.Chaos or campaign-specific extensions), mass file modification events, ransom note drops. Review for unauthorized code-signed binaries with MuddyWater-linked certificate thumbprints as published in Rapid7's campaign analysis.
3. Step 3: Eradication. Remove any unauthorized remote access tools installed during the intrusion period. Reset credentials for all accounts that granted remote access or were present on affected endpoints, prioritizing privileged accounts. Re-image endpoints where remote access was confirmed if full forensic scope cannot be established. Disable any backdoor persistence mechanisms (check T1547 run keys, scheduled tasks, startup folder entries). Block identified C2 infrastructure at the firewall and DNS layer using IOCs from Rapid7's report.
4. Step 4: Recovery. Validate that all remote access tools are removed and no unauthorized scheduled tasks or registry run keys remain. Monitor RDP and lateral movement activity for 30 days post-remediation using enhanced logging. Confirm that no data staging or exfiltration activity continues. Restore affected systems from verified clean backups only after endpoint validation. Re-enable Teams external access only after implementing domain allowlists for approved external tenants.
5. Step 5: Post-Incident. Conduct a user awareness campaign specifically addressing helpdesk impersonation via Teams, including the pattern of external tenant messages requesting remote access. Review and enforce a policy requiring IT staff to initiate remote support sessions, never to accept inbound remote access requests via chat. Evaluate deployment of Microsoft Entra ID Conditional Access policies to restrict remote tool execution. Document the business justification for Teams external access; if no documented requirement exists, disable cross-tenant messaging immediately.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate immediately to legal counsel and executive leadership if forensic evidence confirms data staging or exfiltration of PII, PHI, or intellectual property — MuddyWater's primary objective is espionage, meaning Chaos ransomware deployment may indicate the data-collection phase is already complete and notification obligations under GDPR, HIPAA, or state breach notification laws may be triggered regardless of whether ransomware encryption occurred.
Recovery Notes	Do not restore Teams external access until a documented allowlist of approved external tenant domains is in place and validated against actual business contracts — MuddyWater exploited the default open-external-messaging posture, and restoring that default reestablishes the initial access vector. Maintain enhanced RDP and remote-tool execution logging for a minimum of 30 days post-eradication, as MuddyWater campaigns have demonstrated re-entry attempts after initial remediation when the same social engineering vector remains available. Treat any post-recovery appearance of AnyDesk.exe, DWAgent.exe, or new external Teams threads from unknown tenants as presumptive re-compromise and re-initiate containment procedures immediately.
Forensic Artifacts	Microsoft Purview Unified Audit Log (RecordType: MicrosoftTeams) — preserves the external tenant sender domain, message timestamps, and session initiation events that establish the MuddyWater social engineering entry point; raw JSON export required as parsed CSV loses sender tenant metadata | AnyDesk connection trace logs at %APPDATA%\AnyDesk\ad_svc.trace and %APPDATA%\AnyDesk\connection_trace.txt — record inbound connection IDs, timestamps, and remote IP addresses used by MuddyWater operators during the remote access session | Windows Prefetch files (C:\Windows\Prefetch\) for ANYDESK.EXE-*.pf, DWAGENT.EXE-*.pf, MSRA.EXE-*.pf, and QUICKASSIST.EXE-*.pf — establish first-execution and last-execution timestamps to scope the intrusion window before credentials were reset or systems were re-imaged | Sysmon Event ID 1 (Process Create) logs showing process lineage of AnyDesk.exe or DWAgent.exe spawned from browser or Teams desktop client, and subsequent child processes (cmd.exe, powershell.exe) launched by the remote access tool during the MuddyWater operator session | Windows Security Event Log Event ID 4648 (Logon with Explicit Credentials) and Event ID 4776 (NTLM credential validation) on domain controllers — MuddyWater credential theft during the remote session would produce explicit-credential logon events as stolen credentials were used for lateral RDP movement (MITRE ATT&CK T1078, T1021.001)

Per-Action IR Details

Step 1: Containment — Audit Microsoft Teams external access settings immediately. Restrict or disable cross-tenant external messaging for non-approved domains via the Microsoft Teams Admin Center under 'External Access' policies. Block AnyDesk and DWAgent executables at the endpoint and network perimeter if not business-required. Revoke Quick Assist permissions for non-IT user groups via Intune or Group Policy where feasible.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST CM-7 (Least Functionality), CIS 4.4 (Implement and Manage a Firewall on Servers), CIS 4.5 (Implement and Manage a Firewall on End-User Devices), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Without Intune: Push a GPO to block AnyDesk.exe and DWAgent.exe via Software Restriction Policies (Computer Configuration > Windows Settings > Security Settings > Software Restriction Policies > Additional Rules, deny by path/hash). For Teams external access without admin tooling: use the Teams Admin Center (admin.teams.microsoft.com > Users > External Access) — this is free and browser-based. Export the current external access policy first: run 'Get-CsExternalAccessPolicy' via Teams PowerShell module (free) before making changes to

preserve the pre-incident state.

Evidence: Before modifying any settings, export and preserve: (1) Teams Admin Center external access policy configuration snapshot — document all allowed/blocked domains as-is; (2) Microsoft Purview Unified Audit Log entries for the 30-day window prior to detection, filtered on RecordType 'MicrosoftTeams' — specifically TeamsSessionStarted and MessageCreatedHasLink events from external tenants; (3) AnyDesk connection log at %APPDATA%\AnyDesk\ad_svc.trace and connection_trace.txt; (4) DWAgent installation artifacts at C:\Program Files\DWAgent\ and registry key HKLM\SYSTEM\CurrentControlSet\Services\DWAgent; (5) Quick Assist session logs in Windows Event Log under Microsoft-Windows-RemoteAssistance/Operational.

Step 2: Detection — Review Microsoft Teams audit logs (via Microsoft Purview / Unified Audit Log) for external tenant message threads, especially those referencing IT support, helpdesk, or urgent access requests. Search endpoint logs for Quick Assist (msra.exe, quickassist.exe), AnyDesk (AnyDesk.exe), and DWAgent process execution events. Hunt for RDP lateral movement (Event ID 4624 with LogonType 10, Event ID 1149 in TerminalServices-RemoteConnectionManager). Check for Chaos ransomware indicators: file extension changes (.Chaos or campaign-specific extensions), mass file modification events, ransom note drops. Review for unauthorized code-signed binaries with MuddyWater-linked certificate thumbprints as published in Rapid7's campaign analysis.

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 SIEM: (1) Pull Teams UAL via PowerShell: 'Search-UnifiedAuditLog -StartDate -EndDate -RecordType MicrosoftTeams -Operations MessageCreated,TeamsSessionStarted | Where-Object {$_.AuditData -match "external"}' — pipe to CSV for offline analysis. (2) Deploy Sysmon with SwiftOnSecurity config (github.com/SwiftOnSecurity/sysmon-config) to capture Event ID 1 (Process Create) for AnyDesk.exe, DWAgent.exe, msra.exe, quickassist.exe spawned by Teams.exe or browser processes. (3) Use this Sigma rule concept for RDP hunting: query Windows Security Log with 'Get-WinEvent -LogName Security | Where-Object {$_.Id -eq 4624 -and $_.Message -match "LogonType.*10"}'. (4) For Chaos ransomware file extension enumeration: 'Get-ChildItem -Path C:\ -Recurse -Filter "*.Chaos" -ErrorAction SilentlyContinue' or search for ransom notes named 'read_it.txt' per known Chaos variants.

Evidence: Capture before scoping changes: (1) Microsoft Purview UAL export for MicrosoftTeams RecordType — preserve raw JSON, as parsed exports lose sender tenant domain metadata critical for attributing the MuddyWater-controlled tenant; (2) Windows Security Event Log (Security.evtx) — Event ID 4624 LogonType 10 (RDP network logon) and Event ID 4648 (explicit credential use) on all endpoints where remote access tools were executed; (3) Microsoft-Windows-TerminalServices-RemoteConnectionManager/Operational — Event ID 1149 (RDP authentication success with source IP); (4) Sysmon Event ID 3 (Network Connection) for AnyDesk.exe and DWAgent.exe outbound connections to identify C2 relay infrastructure; (5) VSS shadow copy status — Chaos ransomware variants typically call vssadmin.exe or wbadmin.exe to delete shadow copies, visible in Sysmon Event ID 1 with those process names as indicators of ransomware detonation phase.

Step 3: Eradication — Remove any unauthorized remote access tools installed during the intrusion period. Reset credentials for all accounts that granted remote access or were present on affected endpoints, prioritizing privileged accounts. Re-image endpoints where remote access was confirmed if full forensic scope cannot be established. Disable any backdoor persistence mechanisms (check T1547 run keys, scheduled tasks, startup folder entries). Block identified C2 infrastructure at the firewall and DNS layer using IOCs from Rapid7's report.

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 IA-5 (Authenticator Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to

Dedicated Administrator Accounts), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Without EDR for persistence hunting: Run 'Get-ScheduledTask | Where-Object {$_.TaskPath -notlike "\Microsoft*"} | Select TaskName, TaskPath, @{N="Actions";E={$_.Actions.Execute}}' to enumerate non-Microsoft scheduled tasks. For run key enumeration: 'reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' and 'reg query HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run' on all affected hosts. For startup folder: check '%APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup'. Use Autoruns (Sysinternals, free) for comprehensive persistence visibility — compare against a known-clean baseline image. For C2 blocking without enterprise firewall: push Windows Firewall rules via GPO for identified MuddyWater C2 IPs, and add C2 domains to the hosts file (C:\Windows\System32\drivers\etc\hosts) pointing to 0.0.0.0 as an immediate DNS-layer block.

Evidence: Preserve before eradication: (1) Full forensic image (using FTK Imager free edition or dc3dd) of any endpoint where DWAgent or AnyDesk was confirmed running — MuddyWater operators use these tools for interactive sessions that may leave operator keystrokes or staged data in temp directories; (2) Memory dump (WinPmem, free) of affected systems before re-imaging — credential theft via Quick Assist or RDP sessions may leave LSASS artifacts or injected credential-harvesting tooling in memory; (3) Registry hive exports (HKLM\SYSTEM, HKLM\SOFTWARE, NTUSER.DAT for affected users) to preserve T1547 run key evidence and DWAgent/AnyDesk service registration; (4) Prefetch files from C:\Windows\Prefetch\ for AnyDesk.exe, DWAgent.exe, msra.exe — prefetch timestamps establish first-execution and last-execution times critical for scoping the intrusion window; (5) $MFT (Master File Table) extract using mftdump or Velociraptor (free) to establish file creation timeline for Chaos ransomware payload drops and any staged exfiltration archives.

Step 4: Recovery — Validate that all remote access tools are removed and no unauthorized scheduled tasks or registry run keys remain. Monitor RDP and lateral movement activity for 30 days post-remediation using enhanced logging. Confirm that no data staging or exfiltration activity continues. Restore affected systems from verified clean backups only after endpoint validation. Re-enable Teams external access only after implementing domain allowlists for approved external tenants.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-7 (Software, Firmware, and Information Integrity), NIST AU-6 (Audit Record Review, Analysis, and Reporting), NIST CP-10 (System Recovery and Reconstitution), CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management)

Compensating: Without SIEM for 30-day monitoring: Schedule a daily PowerShell task that queries Security.evtx for Event ID 4624 LogonType 10 and Event ID 4648, exports to a dated CSV, and emails results to the IR team — achievable with Send-MailMessage in a scheduled task. For Teams allowlist validation without automation: weekly manual review of the Teams Admin Center External Access configuration to confirm no new domains have been added. For backup integrity verification: use 'Get-FileHash' (PowerShell built-in) to hash restored critical system binaries against Microsoft's known-good hashes before returning systems to production. Deploy Sysmon persistently post-recovery and forward Event ID 1, 3, and 11 logs to a central share for rolling 30-day retention.

Evidence: Before restoring from backup, verify: (1) Confirm backup creation timestamps predate the MuddyWater initial Teams contact event (establish intrusion start date from UAL TeamsSessionStarted records) — restoring a backup that postdates initial access reintroduces the compromise; (2) Check restored systems for residual AnyDesk or DWAgent registry artifacts using 'reg query HKLM\SYSTEM\CurrentControlSet\Services' before reconnecting to the network; (3) Validate that VSS/shadow copies on recovered systems were not created by Chaos ransomware operators post-encryption and are legitimate pre-incident snapshots; (4) Capture a Sysmon Event ID 7 (Image Loaded) baseline for the first 72 hours post-recovery to detect any DLL side-loading persistence that survived re-imaging if a partial recovery path was taken.

Step 5: Post-Incident — Conduct a user awareness campaign specifically addressing helpdesk impersonation via Teams, including the pattern of external tenant messages requesting remote access. Review and enforce a policy requiring IT staff to initiate remote support sessions — never to accept inbound remote access requests via chat. Evaluate deployment of Microsoft Entra ID Conditional Access policies to restrict remote tool execution. Assess whether your Microsoft Teams external access configuration matches your actual

business need — many organizations leave external messaging open by default without a documented requirement.

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-6 (Configuration Settings), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 6.3 (Require MFA for Externally-Exposed Applications)

Compensating: Without Entra ID P2 licensing for Conditional Access: Use Microsoft Entra ID Free tier to enforce MFA on all admin accounts via Security Defaults (free, enabled in Azure AD portal > Properties > Manage Security Defaults). For awareness training without a budget: create a tabletop exercise scenario using the exact MuddyWater Teams lure pattern — external tenant 'IT helpdesk' message requesting Quick Assist — and walk staff through recognition and reporting procedures; document as a 30-minute team drill. Publish an internal one-page advisory (PDF or intranet post) with a screenshot mock-up of what a MuddyWater-style Teams impersonation message looks like, specifically calling out the external tenant badge indicator that appears on all cross-tenant Teams messages.

Evidence: Document for lessons-learned and policy record: (1) Full timeline from initial MuddyWater Teams contact to ransomware detonation — reconstruct from UAL TeamsSessionStarted timestamps, Quick Assist/AnyDesk first-execution Prefetch timestamps, and Chaos payload drop MFT timestamps to establish dwell time; (2) Scope of credential exposure — list all accounts present on affected endpoints during the intrusion window (from Security Event ID 4624/4648 logs) to confirm password reset completeness; (3) Data staging evidence — review Sysmon Event ID 11 (File Create) for large archive files (.zip, .rar, .7z) created in temp or user directories during the intrusion window, documenting what, if any, data was positioned for exfiltration; (4) Pre-incident Teams external access configuration (exported in Step 1) as the documented baseline for the policy gap finding; (5) IOC set from this campaign (C2 IPs, certificate thumbprints, file hashes) formatted as a STIX bundle or simple CSV for ingestion into future detection tooling.

Detection Guidance

Primary detection focus is on Teams external messaging abuse and unauthorized remote access tool execution. In Microsoft Purview Unified Audit Log, query for TeamsSessionStarted and MessageSent events originating from external tenant domains, filter for messages containing terms such as 'helpdesk', 'IT support', 'remote access', 'Quick Assist', or 'urgent'. On endpoints, alert on execution of quickassist.exe, AnyDesk.exe, and DWAgent.exe, particularly when spawned from user-context processes or following a Teams session. For lateral movement, correlate Windows Security Event ID 4624 (LogonType 10 = RemoteInteractive) with Event ID 4648 (explicit credential use) and TerminalServices-RemoteConnectionManager Event ID 131 across internal hosts. For ransomware deception layer detection, look for high-volume file rename or overwrite events (Sysmon Event ID 11, FileCreate across multiple directories in a short window), creation of ransom note files, and volume shadow copy deletion (vssadmin.exe delete shadows, Event ID 4688 with relevant command line). Hunt for WebView2-based credential harvesting by monitoring for webview2.exe spawned outside of known application contexts. Cross-reference any newly observed code-signed binaries against MuddyWater certificate indicators published by Rapid7.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`Refer to Rapid7 campaign report for specific C2 domains`	MuddyWater C2 infrastructure identified through infrastructure overlap analysis; specific values published in Rapid7 advisory	MEDIUM
HASH	`Refer to Rapid7 campaign report for Chaos ransomware and backdoor hashes`	Code-signed MuddyWater tooling and Chaos ransomware payload; specific hash values published in Rapid7 advisory	MEDIUM
URL	`Refer to Rapid7 campaign report for leak portal URL`	Chaos ransomware-associated data leak portal used as deception layer; specific URL published in Rapid7 advisory	MEDIUM

Framework Mappings

MITRE-ATTACK

- **T1036** — Masquerading
- **T1059.001** — PowerShell
- **T1486** — Data Encrypted for Impact
- **T1560** — Archive Collected Data
- **T1566.004** — Spearphishing Voice
- **T1497** — Virtualization/Sandbox Evasion
- **T1021.001** — Remote Desktop Protocol
- **T1583** — Acquire Infrastructure
- **T1219** — Remote Access Tools
- **T1556** — Modify Authentication Process
- **T1041** — Exfiltration Over C2 Channel
- **T1071.001** — Web Protocols
- **T1036.005** — Match Legitimate Resource Name or Location
- **T1547** — Boot or Logon Autostart Execution
- **T1059.003** — Windows Command Shell
- **T1027** — Obfuscated Files or Information
- **T1078** — Valid Accounts
- **T1588.003** — Code Signing Certificates

NIST-800-53R5

- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **SI-7** — Software, Firmware, and Information Integrity

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **AC-2** — Account Management
- **IA-8** — Identification and Authentication (Non-Organizational Users)
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan
- **SC-13** — Cryptographic Protection

OWASP-TOP10-2021

- **A07:2021** — Identification and Authentication Failures
- **A04:2021** — Insecure Design

CIS-V8

- **6.3** — Require MFA for Externally-Exposed Applications
- **6.4** — Require MFA for Remote Network Access
- **6.5** — Require MFA for Administrative Access
- **5.2** — Use Unique Passwords
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC9.2** — Manages risks associated with vendors and business partners

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1036	Masquerading	Defense-Evasion
T1059.001	PowerShell	Execution
T1486	Data Encrypted for Impact	Impact
T1560	Archive Collected Data	Collection
T1566.004	Spearphishing Voice	Initial-Access
T1497	Virtualization/Sandbox Evasion	Defense-Evasion
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1583	Acquire Infrastructure	Resource-Development
T1219	Remote Access Tools	Command-And-Control
T1556	Modify Authentication Process	Credential-Access
T1041	Exfiltration Over C2 Channel	Exfiltration
T1071.001	Web Protocols	Command-And-Control
T1036.005	Match Legitimate Resource Name or Location	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1059.003	Windows Command Shell	Execution
T1027	Obfuscated Files or Information	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1588.003	Code Signing Certificates	Resource-Development

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/muddywater-hackers-u...	T3
Microsoft: Teams increasingly abused in helpdesk impersonation ...	https://www.reddit.com/r/cybersecurity/comments/1sqx3i2/microsoft_t...	T3

Source	URL	Tier
Cross■tenant helpdesk impersonation to data exfiltration - Microsoft	https://www.microsoft.com/en-us/security/blog/2026/04/18/crosstenan...	T1
Microsoft issues warning over Teams helpdesk impersonation attacks	https://www.techradar.com/pro/security/microsoft-issues-warning-ove...	T3
Microsoft Teams, Quick Assist weaponized in helpdesk spoofing ...	https://www.scworld.com/brief/microsoft-teams-quick-assist-weaponiz...	T3

Generated 2026-05-06 18:52 UTC by TJS Security Command Center