INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-23 18:50 UTC

UNC6692 Builds Modular Attack Chain Around Teams Helpdesk Impersonation and Custom SNOW Malware Suite

THREAT CAMPAIGN | **HIGH** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0211
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	9.5
Affected Products	Microsoft Teams, Microsoft Edge, Windows (LSASS, cmd.exe, PowerShell), Quick Assist, Supremo Remote Desktop, FTK Imager, AWS S3
Published	2026-04-23T14:16:00
Discovery Source	Rss

Executive Summary

A newly identified threat group, UNC6692, is conducting targeted social engineering attacks against enterprise employees by impersonating IT helpdesk staff through Microsoft Teams. Attackers use email bombing to overwhelm targets, then call via Teams posing as support, gaining remote access through Microsoft Quick Assist before deploying a custom three-component malware suite. The campaign is assessed as a direct precursor to ransomware deployment and Active Directory compromise, with 77% of observed incidents targeting senior-level employees between March and April 2026.

Technical Analysis

UNC6692 executes a multi-stage intrusion chain beginning with email bombing followed by unsolicited Teams calls impersonating internal IT helpdesk. The actor abuses Microsoft Quick Assist (T1219) and Supremo Remote Desktop to establish initial remote access without exploiting a traditional vulnerability. Post-access activity includes deployment of three previously undocumented malware components: SNOWBELT, SNOWGLAZE, and SNOWBASIN. Credential harvesting targets LSASS memory via FTK Imager abuse (T1003.001) and NTDS exfiltration (T1003.003). Lateral movement uses PsExec over SMB (T1021.002) and Pass-the-Hash (T1550.002). C2 and payload staging leverage AWS S3 buckets (T1567, T1102) with WebSocket-based C2 communication (T1071.001), exploiting trusted cloud infrastructure to bypass reputation-based network controls. Persistence mechanisms (T1547) and sandbox evasion (T1497) are incorporated into the SNOW malware suite. Browser extension abuse (T1176) and internal spearphishing

(T1534) extend the actor's reach post-compromise. Relevant CWEs: CWE-290 (Authentication Bypass by Spoofing), CWE-308 (Single-Factor Authentication), CWE-522 (Insufficiently Protected Credentials). No CVE is associated, the campaign exploits legitimate tool abuse and social engineering, not unpatched software vulnerabilities. Primary source: Microsoft Security Blog, March 16, 2026.

Action Checklist

1. Containment, Disable or restrict Microsoft Quick Assist across the enterprise via Group Policy (set QuickAssistEnabled to 0 [disabled]) if remote support can be handled through an approved, monitored alternative. Block Supremo Remote Desktop executables and installer hashes at the endpoint and perimeter. Restrict outbound WebSocket connections to AWS S3 endpoints not on an approved allow-list.
2. Detection, Review Microsoft Teams call logs for external accounts initiating unsolicited calls to employees, particularly senior staff. Search endpoint EDR telemetry for FTK Imager execution, LSASS memory access from non-system processes, and PowerShell or cmd.exe spawning from Quick Assist or Supremo parent processes. Query SIEM for high-volume inbound email delivery to single mailboxes within short windows (email bombing precursor pattern). Audit AWS S3 traffic from endpoints for unexpected bucket access, particularly for PUT or GET operations outside approved cloud services.
3. Eradication, Remove SNOWBELT, SNOWGLAZE, and SNOWBASIN components identified through EDR scans; reference Microsoft Security Blog (March 16, 2026) for component behavioral signatures. Revoke and reset credentials for any account where LSASS access or NTDS exfiltration is confirmed. Rotate all Active Directory service account credentials and Kerberos tickets (krbtgt double-reset) if domain-level access is suspected. Terminate unauthorized remote access sessions and remove persistence mechanisms identified under T1547 (registry run keys, scheduled tasks).
4. Recovery, Validate Active Directory integrity: audit privileged group membership, GPO modifications, and new accounts created during the incident window. Re-enable MFA enforcement across all accounts, prioritizing senior staff and IT administrators. Monitor for Pass-the-Hash activity (T1550.002) and lateral SMB connections from previously compromised hosts for a minimum of 30 days post-remediation. Confirm no rogue browser extensions (T1176) remain on affected endpoints.
5. Post-Incident, Conduct targeted security awareness training for senior employees and IT support staff focused on Teams-based social engineering and unsolicited remote access requests. Implement a verified callback procedure for all IT helpdesk-initiated remote access sessions. Review and enforce conditional access policies requiring MFA for all remote access tools. Evaluate network controls to restrict outbound connections to unapproved cloud storage endpoints, addressing the trusted-infrastructure evasion technique central to this campaign.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to senior leadership, legal counsel, and potentially law enforcement if LSASS dumping (confirmed via Sysmon Event ID 10) or NTDS.dit exfiltration is confirmed on any domain controller, if Active Directory privileged group membership has been modified by UNC6692-created accounts, if regulated data (PII, PHI, PCI) is stored on systems accessed via the Quick Assist or Supremo sessions (triggering breach notification timelines under GDPR 72-hour, HIPAA 60-day, or applicable state law requirements), or if the incident response team lacks Active Directory forensics capability to perform the krbtgt double-reset and privileged account audit without risking further compromise.
Recovery Notes	Post-containment recovery must begin with a verified Active Directory baseline — do not restore any systems to production until the krbtgt double-reset is complete (both resets confirmed with a 10-hour interval), all UNC6692-created accounts are removed, and no unauthorized GPO modifications remain in SYSVOL. Monitor all previously compromised endpoints and any hosts that received lateral SMB connections for Pass-the-Hash (Windows Security Event ID 4624 Type 3 with NtLmSsp) and Kerberos ticket anomalies (Event ID 4769 with unusual SPN targets) for a minimum of 30 days, given UNC6692's assessed intent as a ransomware precursor group with established AD persistence tradecraft. Re-validate MFA enforcement for all accounts — particularly senior staff and IT administrators who were the primary social engineering targets — using Azure AD Sign-In logs to confirm no MFA bypass conditions (legacy authentication protocols, conditional access exclusions) remain active before declaring full recovery.
Forensic Artifacts	Microsoft-Windows-RemoteAssistance/Operational event log (Event IDs 200, 201) and %LOCALAPPDATA%\Temp\QuickAssist\ log files recording the UNC6692 operator's connecting IP, session GUID, and duration — the primary attribution artifact linking the remote access session to the SNOW* malware deployment chain. | Sysmon Event ID 10 (ProcessAccess) entries targeting lsass.exe with GrantedAccess codes 0x1010 or 0x1410, attributed to FTK Imager or SNOWGLAZE — these specific handle access masks are the forensic signature of memory-based credential extraction as used by UNC6692 rather than generic LSASS read activity. | Supremo connection log at %APPDATA%\Supremo\Log\SupremoLog.txt recording the UNC6692 operator's remote IP, file transfer events (used to stage SNOWBELT, SNOWGLAZE, SNOWBASIN), and session timestamps that establish the precise window between initial Teams social engineering contact and malware deployment. | Windows Security Event ID 4769 (Kerberos Service Ticket Requests) and 4648 (Explicit Credential Use) logs from the compromised host showing DCSync or Pass-the-Hash lateral movement attempts following LSASS credential extraction — these establish whether UNC6692 progressed beyond initial access toward Active Directory compromise and ransomware pre-positioning. | Network capture or Windows Firewall Event ID 5156 logs showing outbound WebSocket or HTTPS connections from SNOW* components to amazonaws.com bucket hostnames, including the specific bucket name (a key IOC for cross-organizational threat intelligence sharing and attribution to UNC6692's AWS-hosted C2 infrastructure).

Per-Action IR Details

Containment — Disable or restrict Microsoft Quick Assist across the enterprise via Group Policy (set 'QuickAssistEnabled' to disabled) if remote support can be handled through an approved, monitored alternative. Block Supremo Remote Desktop executables and installer hashes at the endpoint and perimeter. Restrict outbound WebSocket connections to AWS S3 endpoints not on an approved allow-list.

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: Deploy the following GPO registry key immediately via Group Policy or manual registry push to disable Quick Assist: HKLM\SOFTWARE\Policies\Microsoft\Windows\QuickAssist — set 'QuickAssistEnabled' DWORD to 0. For Supremo, extract the SHA-256 hash of Supremo.exe from a known-bad sample and add it to Windows Defender's controlled folder access block list using PowerShell: Add-MpPreference -ExclusionPath is insufficient — instead use: Set-MpPreference -AttackSurfaceReductionRules_Ids -AttackSurfaceReductionRules_Actions Enabled. For S3 WebSocket egress without a SIEM, configure Windows Firewall (netsh advfirewall or PowerShell New-NetFirewallRule) to block outbound TCP 443 to amazonaws.com subnets not on your approved list; obtain current AWS IP ranges from https://ip-ranges.amazonaws.com/ip-ranges.json and parse with a one-liner: Invoke-RestMethod https://ip-ranges.amazonaws.com/ip-ranges.json | Select-Object -ExpandProperty prefixes | Where-Object {$_.service -eq 'S3'} | Select-Object ip_prefix.

Evidence: Before disabling Quick Assist, capture the Windows Event Log 'Microsoft-Windows-TerminalServices-LocalSessionManager/Operational' for session initiation events and 'Microsoft-Windows-RemoteAssistance/Operational' (Event IDs 200, 201) recording the remote session GUID, connecting IP, and timestamp. Export Quick Assist connection history from %LOCALAPPDATA%\Temp\QuickAssist\ and %APPDATA%\Microsoft\QuickAssist\logs\. For Supremo, collect the Supremo connection log at %APPDATA%\Supremo\Log\SupremoLog.txt which records remote IP, session duration, and file transfers. Capture current outbound NetFlow or Windows Firewall logs (Event ID 5156 — network connection allowed) filtered on amazonaws.com destinations before blocking, to establish the full C2 beacon timeline for SNOWBELT or SNOWGLAZE exfiltration channels.

Detection — Review Microsoft Teams call logs for external accounts initiating unsolicited calls to employees, particularly senior staff. Search endpoint EDR telemetry for FTK Imager execution, LSASS memory access from non-system processes, and PowerShell or cmd.exe spawning from Quick Assist or Supremo parent processes. Query SIEM for high-volume inbound email delivery to single mailboxes within short windows (email bombing precursor pattern). Audit AWS S3 traffic from endpoints for unexpected bucket access, particularly for PUT or GET operations outside approved cloud services.

NIST Phase: Detection Analysis

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

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

Compensating: For Teams call log review without a SIEM, pull the Microsoft Teams Admin Center > Analytics & Reports > PSTN and Teams call logs via PowerShell using the MicrosoftTeams module: Get-CsUserSession -UserPrincipalName and filter on ExternalCallerIdName or CallerNumber matching non-tenant domains. For LSASS access detection without EDR, deploy Sysmon with the SwiftOnSecurity config and query Event ID 10 (ProcessAccess) where TargetImage contains 'lsass.exe' and GrantedAccess matches 0x1010 or 0x1410 (common Mimikatz/FTK Imager read handles): sysmon -s to dump current config and validate rule coverage. For FTK Imager specifically, query Sysmon Event ID 1 (Process Creation) for CommandLine containing 'ftkimager' or 'AD1' file output arguments. For email bombing detection without a SIEM, run the following Exchange Online PowerShell query: Get-MessageTrace -RecipientAddress -StartDate (Get-Date).AddHours(-24) -EndDate (Get-Date) | Group-Object SenderAddress | Sort-Object Count -Descending | Select-Object -First 20. For S3 PUT/GET detection, use Wireshark or tcpdump on a network tap filtering on 'host s3.amazonaws.com and (tcp.flags.push == 1)' and inspect HTTP Host headers for unexpected bucket names.

Evidence: Capture Microsoft Teams Unified Audit Log entries (Office 365 Management Activity API, RecordType=MicrosoftTeams, Operation=CallStarted or MessageSent) for the 72-hour window preceding the first reported social engineering contact, specifically filtering on CommunicationType='External'. Collect Sysmon Event ID 10 logs showing LSASS handle access with GrantedAccess codes 0x1010, 0x1410, or 0x143A — these are the specific access masks FTK Imager requests when imaging LSASS memory for credential extraction. Preserve Windows Security Event ID 4688 (Process Creation) showing the parent-child process chain: QuickAssist.exe or Supremo.exe spawning cmd.exe, powershell.exe, or any SNOW* component binary. Collect Exchange/M365 message trace logs showing the email bombing pattern (>50 inbound messages to a single recipient within a 10-minute window)

which UNC6692 uses as the social engineering entry trigger. Export DNS query logs or Windows Event ID 5156/5158 entries showing outbound resolution and connections to amazonaws.com bucket hostnames not matching approved corporate cloud services.

Eradication — Remove SNOWBELT, SNOWGLAZE, and SNOWBASIN components identified through EDR scans; reference Microsoft Security Blog (March 16, 2026) for component behavioral signatures. Revoke and reset credentials for any account where LSASS access or NTDS exfiltration is confirmed. Rotate all Active Directory service account credentials and Kerberos tickets (krbtgt double-reset) if domain-level access is suspected. Terminate unauthorized remote access sessions and remove persistence mechanisms identified under T1547 (registry run keys, scheduled tasks).

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-7 (Software, Firmware, and Information Integrity), NIST IA-5 (Authenticator Management), CIS 5.3 (Disable Dormant Accounts), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For SNOWBELT, SNOWGLAZE, and SNOWBASIN removal without EDR, write YARA rules based on the behavioral signatures published in the Microsoft Security Blog (March 16, 2026) and scan with: yara64.exe -r C:\ targeting known UNC6692 staging directories (%TEMP%, %APPDATA%\Microsoft\, %PROGRAMDATA%). For registry persistence (T1547.001), enumerate run keys with: reg query HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run and HKCU equivalent — remove any entries pointing to non-standard paths or unsigned binaries. For scheduled tasks, run: schtasks /query /fo LIST /v | findstr /i "TaskName Status Run As Program" and cross-reference against your approved baseline. For the krbtgt double-reset, execute the reset twice with a 10-hour interval (exceeding the default Kerberos ticket lifetime) using the Microsoft New-KrbtgtKeys.ps1 script to ensure all previously issued TGTs are invalidated — this is mandatory if NTDS.dit exfiltration via SNOWBASIN is suspected. For NTDS exfiltration confirmation, check Volume Shadow Copy Service logs and run: vssadmin list shadows and verify no unauthorized VSS snapshots were created by non-system processes (a common NTDS.dit extraction precursor).

Evidence: Before removing SNOW* components, collect full memory dumps of affected processes using ProcDump (Sysinternals): procdump.exe -ma — preserving in-memory indicators of SNOWGLAZE's C2 communication state and SNOWBELT's credential harvest buffer. Image the %TEMP% and %APPDATA%\Microsoft directories with FTK Imager (ironic given UNC6692's use of the same tool) or using robocopy /MIR to a forensic share before deletion, preserving file creation timestamps and NTFS MFT entries. Collect Windows Security Event ID 4648 (explicit credential logon) and 4624 Type 9 (NewCredentials) logs showing Pass-the-Hash or Pass-the-Ticket lateral movement originating from the initially compromised host. Capture ntdsutil or VSS activity from Windows Event ID 7036 (Service Control Manager) and Security Event 4699 (scheduled task deleted) to document UNC6692's NTDS extraction method. Export the full Active Directory replication metadata using repadmin /showrepl and Get-ADReplicationFailure to identify any unauthorized DC sync operations (DCSync — T1003.006) performed by SNOWBASIN.

Recovery — Validate Active Directory integrity: audit privileged group membership, GPO modifications, and new accounts created during the incident window. Re-enable MFA enforcement across all accounts, prioritizing senior staff and IT administrators. Monitor for Pass-the-Hash activity (T1550.002) and lateral SMB connections from previously compromised hosts for a minimum of 30 days post-remediation. Confirm no rogue browser extensions (T1176) remain on affected endpoints.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST IA-5 (Authenticator Management), NIST AC-2 (Account Management), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: For AD integrity validation without a commercial tool, run the following PowerShell sequence: (1) Get-ADGroupMember 'Domain Admins' | Select-Object Name,SamAccountName,WhenCreated — filter for accounts

created during the incident window; (2) Get-GPO -All | Get-GPOReport -ReportType XML | Select-String -Pattern 'ModifiedTime' to identify GPOs modified during the attack window; (3) Get-ADUser -Filter {WhenCreated -gt ''} -Properties WhenCreated,LastLogonDate to find backdoor accounts. For rogue Edge browser extension detection (T1176) without EDR, audit the extension registry at HKCU\SOFTWARE\Microsoft\Edge\Extensions and compare against an approved extension allowlist; additionally inspect %LOCALAPPDATA%\Microsoft\Edge\User Data\Default\Extensions\ for directory creation timestamps within the incident window. For Pass-the-Hash monitoring without a SIEM, configure a Sigma rule targeting Windows Security Event ID 4624 (Type 3 logon with NtLmSsp authentication package) originating from previously compromised host IPs using a scheduled PowerShell query: Get-WinEvent -FilterHashtable @{LogName='Security';Id=4624} | Where-Object {$_.Message -match 'NtLmSsp' -and $_.Message -match ''}.

Evidence: Before declaring recovery complete, collect a point-in-time snapshot of Active Directory privileged group membership using Get-ADGroupMember for Domain Admins, Enterprise Admins, Schema Admins, and any custom-named admin groups — compare against the pre-incident baseline to identify UNC6692-created persistence accounts. Export Group Policy Object change history from the SYSVOL GPT.INI version counters (SYSVOL\\Policies\\GPT.INI — version number increments on each GPO edit) to identify GPOs modified by UNC6692 for potential privilege escalation or policy weakening. Collect Microsoft Edge extension manifest files (manifest.json) from all affected endpoints, specifically examining 'permissions' fields for webRequest, tabs, or storage access that would indicate SNOWGLAZE's browser-based credential harvesting capability (T1176). Preserve Windows Security Event ID 4769 (Kerberos Service Ticket Request) logs showing ticket requests for sensitive SPNs (CIFS, HOST, LDAP on domain controllers) from hosts outside their normal operational pattern, indicating post-krbtgt-reset validation of ticket invalidation effectiveness.

Post-Incident — Conduct targeted security awareness training for senior employees and IT support staff focused on Teams-based social engineering and unsolicited remote access requests. Implement a verified callback procedure for all IT helpdesk-initiated remote access sessions. Review and enforce conditional access policies requiring MFA for all remote access tools. Evaluate network controls to restrict outbound connections to unapproved cloud storage endpoints, addressing the trusted-infrastructure evasion technique central to this campaign.

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 SI-5 (Security Alerts, Advisories, and Directives), NIST AU-6 (Audit Record Review, Analysis, and Reporting), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.4 (Require MFA for Remote Network Access), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: For the verified callback procedure without a commercial ticketing system, implement a shared Teams channel (internal-only, not federated) where IT staff post a pre-approved support code before initiating any remote session — employees are trained to verify the code in the internal channel before accepting any Quick Assist or remote tool request. For conditional access policy enforcement without Azure AD P2, use Azure AD Free Conditional Access baselines to enforce MFA for all admin roles and configure Microsoft Teams external access policies via PowerShell: Set-CsTenantFederationConfiguration -AllowPublicUsers $false and Set-CsExternalAccessPolicy -EnableFederationAccess $false for high-risk user groups. For S3 egress restriction without a next-gen firewall, use Windows Firewall GPO with outbound rules blocking TCP 443 to the full amazonaws.com IP range minus approved buckets, parsed from the AWS IP range JSON file on a weekly automated basis using a scheduled PowerShell task. Document UNC6692 IOCs (SNOW* component hashes, Supremo installer hashes, AWS S3 bucket names used for C2) in a local MISP instance (free, open source) or a structured threat intel SharePoint list to feed future detection rules.

Evidence: Document the complete UNC6692 attack chain timeline reconstructed from: Teams call logs (external caller ID and timestamp), email bombing delivery records from Exchange message trace, Quick Assist session GUIDs correlated with Supremo connection logs, LSASS access event IDs and associated process handles, SNOW* component execution timestamps from Sysmon Event ID 1, and AWS S3 PUT/GET connection records — this unified timeline is the primary artifact for the lessons-learned report and regulatory notification assessment. Preserve all EDR

telemetry, Sysmon logs, Windows Security event logs, and network flow data under litigation hold for a minimum of 12 months given the ransomware precursor classification and potential regulatory notification obligations. Capture the final Active Directory state report (privileged groups, GPO versions, new accounts, Kerberos policy settings) post-krbtgt reset as the validated recovery baseline against which future AD audits will be compared.

Detection Guidance

Key detection opportunities span three layers. At the email gateway: alert on delivery of 50 or more emails to a single recipient within a 10-minute window, which is the email bombing precursor UNC6692 uses to manufacture a pretext for the helpdesk call. In Microsoft Teams audit logs (available via Microsoft Purview): flag external-tenant accounts initiating voice or video calls to internal users who have no prior communication history with that account, particularly calls originating from accounts with generic display names mimicking IT support. At the endpoint via EDR: create rules for FTK Imager execution (ftkimager.exe) outside authorized forensic workflows; LSASS memory access (T1003.001) from processes other than known system processes; PowerShell (T1059.001) or cmd.exe (T1059.003) spawned as child processes of Quick Assist (quickassist.exe) or Supremo (Supreme.exe); and outbound connections from those same parent processes to AWS S3 domains (*.s3.amazonaws.com) not on an approved list. For network detection: alert on WebSocket connections (wss://) to AWS S3 endpoints from endpoint hosts, which represents the C2 channel (T1071.001). MITRE ATT&CK coverage priorities: T1219, T1003.001, T1003.003, T1550.002, T1567, T1071.001. No public IOC list has been confirmed in the item data; reference the Microsoft Security Blog (March 16, 2026) for any hashes or infrastructure indicators released by Microsoft.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`*.s3.amazonaws.com`	AWS S3 buckets used for payload staging, C2 communication, and credential exfiltration — network connections to S3 from endpoints outside approved cloud services warrant investigation	MEDIUM
URL	`https://www.microsoft.com/en-us/security/blog/2026/03/16/help-on-the-line-how-a-microsoft-teams-support-call-led-to-compromise/`	Microsoft Security Blog primary technical analysis — refer here for any specific hashes, infrastructure indicators, or SNOW malware signatures released by Microsoft	HIGH

Framework Mappings

MITRE-ATTACK

- **T1567** — Exfiltration Over Web Service
- **T1078** — Valid Accounts
- **T1059.003** — Windows Command Shell
- **T1003.001** — LSASS Memory

- **T1071.001** — Web Protocols
- **T1566.004** — Spearphishing Voice
- **T1021.002** — SMB/Windows Admin Shares
- **T1041** — Exfiltration Over C2 Channel
- **T1003.003** — NTDS
- **T1550.002** — Pass the Hash
- **T1547** — Boot or Logon Autostart Execution
- **T1059.001** — PowerShell
- **T1046** — Network Service Discovery
- **T1027** — Obfuscated Files or Information
- **T1102** — Web Service
- **T1497** — Virtualization/Sandbox Evasion
- **T1566** — Phishing
- **T1219** — Remote Access Tools
- **T1021.001** — Remote Desktop Protocol
- **T1486** — Data Encrypted for Impact
- **T1176** — Software Extensions
- **T1656** — Impersonation
- **T1105** — Ingress Tool Transfer
- **T1534** — Internal Spearphishing
- **T1598** — Phishing for Information

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-7** — Software, Firmware, and Information Integrity
- **AT-2** — Literacy Training and Awareness
- **SI-8** — Spam Protection
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **IR-4** — Incident Handling
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

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

CIS-V8

- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **14.2** — Train Workforce Members to Recognize Social Engineering Attacks
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

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

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **GV.SC-01** — Cybersecurity supply chain risk management program
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.21** — Managing information security in the ICT supply chain
- **A.5.23** — Information security for use of cloud services

SOC2-TSC

- **CC6.1** — Logical access security software, infrastructure, and architectures
- **CC9.2** — Manages risks associated with vendors and business partners

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1567	Exfiltration Over Web Service	Exfiltration
T1078	Valid Accounts	Defense-Evasion
T1059.003	Windows Command Shell	Execution
T1003.001	LSASS Memory	Credential-Access
T1071.001	Web Protocols	Command-And-Control
T1566.004	Spearphishing Voice	Initial-Access

Technique ID	Technique Name	Tactic
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1041	Exfiltration Over C2 Channel	Exfiltration
T1003.003	NTDS	Credential-Access
T1550.002	Pass the Hash	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1059.001	PowerShell	Execution
T1046	Network Service Discovery	Discovery
T1027	Obfuscated Files or Information	Defense-Evasion
T1102	Web Service	Command-And-Control
T1497	Virtualization/Sandbox Evasion	Defense-Evasion
T1566	Phishing	Initial-Access
T1219	Remote Access Tools	Command-And-Control
T1021.001	Remote Desktop Protocol	Lateral-Movement
T1486	Data Encrypted for Impact	Impact
T1176	Software Extensions	Persistence
T1656	Impersonation	Defense-Evasion
T1105	Ingress Tool Transfer	Command-And-Control
T1534	Internal Spearphishing	Lateral-Movement
T1598	Phishing for Information	Reconnaissance

Sources

Source	URL	Tier
Security News	https://thehackernews.com/2026/04/unc6692-impersonates-it-helpdesk-...	T3
Microsoft issues warning over Teams helpdesk impersonation attacks	https://www.techradar.com/pro/security/microsoft-issues-warning-ove...	T3

Source	URL	Tier
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
Fake Helpdesk Attack Uses Teams and Quick Assist to Breach Targets	https://www.linkedin.com/posts/lewiscombs_fake-helpdesk-attack-uses...	T3
Signed malware impersonating workplace apps deploys RMM ...	https://www.microsoft.com/en-us/security/blog/2026/03/03/signed-mal...	T1

Generated 2026-04-23 18:50 UTC by TJS Security Command Center