INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-06-22 13:57 UTC

Parallel Threat Actor Intrusion: Storm-2603 and Unattributed Actor Simultaneously Compromise Shared Environment

THREAT CAMPAIGN | **HIGH** | CVSS 7.5

SCC Item ID	SCC-CAM-2026-0534
Type	Threat Campaign
Severity	HIGH
CVSS Base Score	7.5
Affected Products	Microsoft SharePoint (on-premises), Visual Studio Code, Cloudflare Tunnel, Zoho Assist
Published	2026-06-22T16:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

Microsoft's Detection and Response Team investigated a ransomware incident and discovered two unrelated threat actors operating simultaneously inside the same compromised environment. Storm-2603 exploited on-premises Microsoft SharePoint servers and used legitimate remote access tools to maintain persistence, while a second unidentified actor ran DLL sideloading and custom backdoors concurrently. The concurrent activity created investigative blind spots that allowed both intrusions to persist longer than a single-actor incident would have, and exposes a structural gap in how most security teams scope and triage incidents.

Technical Analysis

Microsoft DART documented a dual-actor intrusion originating from exploitation of on-premises Microsoft SharePoint servers (CVE details tracked in associated Microsoft advisories; see source URLs). Storm-2603 established persistence through Visual Studio Code remote tunneling, Cloudflare Tunnel, and Zoho Assist for remote access, all legitimate tools that evade signature-based endpoint detection. The actor also used a Bring Your Own Vulnerable Driver (BYOVD) technique (MITRE T1068) to disable endpoint defenses. A second, unattributed actor operated concurrently using DLL sideloading (T1574.002) and custom backdoors (T1505.003). Relevant CWEs: CWE-284 (Improper Access Control), CWE-912 (Hidden Functionality/backdoor behavior), CWE-269 (Improper Privilege Management). MITRE techniques observed span initial access via public-facing exploitation (T1190), valid account abuse (T1078, T1078.002), command execution (T1059), SSH tunneling (T1021.004), local and domain account creation (T1136.001, T1136.002), indicator removal (T1070),

defense evasion via masquerading (T1036) and impair defenses (T1562.001), service persistence (T1543), and protocol tunneling (T1572). No public CVE ID is embedded in the item data; consult the Microsoft Security Blog and Cyberattack Series Report No. 9 for specific SharePoint vulnerability identifiers. Patch status: Microsoft has published guidance on disrupting active SharePoint exploitation (see source: disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities).

Action Checklist

1. Step 1: Containment. Immediately isolate on-premises SharePoint servers showing anomalous outbound connections, particularly to Cloudflare Tunnel endpoints, VS Code tunnel infrastructure, or Zoho Assist relay services. Block outbound traffic on ports used by these tools at the perimeter firewall until legitimacy is confirmed. Reference NIST AC-4 (Information Flow Enforcement) for flow restriction authority.
2. Step 2: Detection. Do not assume a single threat actor. Assign independent triage threads to each distinct behavioral cluster observed in logs. Query endpoint and network logs for concurrent anomalies: (a) VS Code tunnel process spawning from SharePoint worker processes (w3wp.exe), (b) Cloudflare Tunnel (cloudflared.exe) running on servers where it has no change-managed justification, (c) Zoho Assist remote session initiation outside business hours, (d) DLL sideloading indicators, unexpected DLLs loaded by signed binaries in non-standard paths, (e) vulnerable driver load events in Windows Security event logs (Event ID 7045 for new service installs; correlate with known BYOVD driver hashes from LOLBAS/LOLDrivers lists). Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs) to ensure log sources are intact and queryable. Flag any gaps in audit coverage immediately.
3. Step 3: Eradication. Apply all current Microsoft patches for on-premises SharePoint as documented in the Microsoft Security Blog advisory (https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active-exploitation-of-on-premises-sharepoint-vulnerabilities/). Remove unauthorized accounts created during the intrusion (audit via T1136.001/T1136.002 indicators). Revoke and rotate all credentials for accounts present on affected SharePoint servers (NIST AC-2, Account Management; D3-CRO, Credential Rotation). Unload and block vulnerable drivers identified in BYOVD activity. Remove unauthorized remote access tooling (VS Code tunnel, cloudflared, Zoho Assist) from servers where no change record exists.
4. Step 4: Recovery. Before restoring SharePoint to production, validate: (a) all identified backdoors and sideloaded DLLs are removed, (b) no unauthorized scheduled tasks or services persist (audit via T1543 indicators), (c) endpoint defenses are fully operational and not impaired (T1562.001 reversal confirmed), (d) a fresh credential rotation is complete for all privileged accounts. Monitor post-restoration for re-emergence of tunneling tool processes and new local account creation. Apply NIST AU-9 (Protection of Audit Information) to confirm logs have not been tampered with during recovery. Reference D3-LAM (Local Account Monitoring) for ongoing account surveillance.
5. Step 5: Post-Incident. Conduct a structured review of triage methodology. Assess whether your SOC playbooks assume single-actor intrusions and update scoping checklists to require explicit multi-actor hypothesis testing on every significant incident. Implement detection rules that flag behavioral clusters independently rather than correlating all activity to the first identified actor. Review whether BYOVD driver blocks (via Windows Defender Vulnerable Driver Blocklist or equivalent) are current. Map control gaps to NIST AC-6 (Least Privilege) and AC-5 (Separation of Duties) to reduce the blast radius of future SharePoint compromises. Reference D3-CH (Credential Hardening) and D3-MFA (Multi-factor Authentication) for persistent access hardening.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to senior IR leadership and legal/compliance if forensic evidence confirms data exfiltration from SharePoint (e.g., bulk document download activity in ULS logs or IIS access logs preceding tunnel establishment), if PII or regulated data was accessible to the compromised SharePoint service account, or if the SOC cannot definitively deconflict the two actor clusters and rule out a third undetected intrusion — active blind spots in a ransomware-adjacent campaign require executive decision authority on isolation scope and breach notification obligations.
Recovery Notes	Restore SharePoint to production only from a known-clean backup predating the earliest confirmed indicator of compromise — do not restore from a snapshot taken during the active intrusion window, as both actors may have implanted persistence in the SharePoint database or web application files. Post-restoration, maintain enhanced monitoring for a minimum of 30 days watching specifically for re-emergence of cloudflared.exe, code.exe in tunnel mode, or ZohoAssist.exe on SharePoint servers, new local account creation (Windows Security Event ID 4720), and DLL Image Load events (Sysmon Event ID 7) from unexpected paths. Given that both actors operated concurrently and the full scope of the unattributed actor's backdoor may not be fully characterized, treat any anomalous outbound HTTPS connection from SharePoint servers as a potential re-compromise indicator requiring immediate triage rather than standard change-management review.
Forensic Artifacts	IIS access logs and SharePoint ULS logs (C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\LOGS\) — review for exploit-indicative POST requests to SharePoint API endpoints (/_vti_bin/, /_layouts/, /sites/) that immediately precede w3wp.exe spawning child processes, establishing the initial Storm-2603 access vector and timeline anchor | Windows Sysmon Event ID 7 (Image Loaded) logs — specific to the unattributed actor's DLL sideloading chain; capture DLL names, full paths, loading process names, and SHA256 hashes for DLLs loaded from non-standard directories (C:\ProgramData, C:\Users\Public, or the SharePoint web root) by Microsoft-signed binaries | Windows System Event Log Event ID 7045 (New Service Installed) entries — specific to BYOVD activity; extract driver service names, binary paths, and compute SHA256 hashes for cross-reference against the LOLDrivers database to identify the specific vulnerable driver used to disable endpoint defenses | Prefetch files (C:\Windows\Prefetch\CLOUDFLARED.EXE-*.pf, CODE.EXE-*.pf, ZOHOASSIST.EXE-*.pf) — provide first-execution timestamps for each tunneling tool independently, enabling reconstruction of which actor established persistence first and whether the tools were installed before or after BYOVD driver loading | Memory forensics from w3wp.exe process dump — extract injected shellcode, in-memory .NET assemblies, or reflectively loaded DLLs that Storm-2603 may have loaded directly into the SharePoint worker process without touching disk, which would be invisible to file-system-based artifact collection alone

Per-Action IR Details

Step 1: Containment — Immediately isolate on-premises SharePoint servers showing anomalous outbound connections, particularly to Cloudflare Tunnel endpoints, VS Code tunnel infrastructure, or Zoho Assist relay services. Block outbound traffic on ports used by these tools at the perimeter firewall until legitimacy is confirmed. Reference NIST AC-4 (Information Flow Enforcement) for flow restriction authority.

NIST Phase: Containment

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

Controls: NIST AC-4 (Information Flow Enforcement), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: On the SharePoint server, run 'netstat -ano | findstr ESTABLISHED' and 'Get-NetTCPConnection | Where-Object {$_.State -eq "Established"}' to enumerate active outbound sessions before blocking. Apply Windows Firewall outbound rules via 'netsh advfirewall firewall add rule' to block ports 443/TCP to known Cloudflare Tunnel CIDR ranges (198.41.128.0/17, 162.158.0.0/15), VS Code tunnel relay endpoints (*.vscode-cdn.net), and Zoho Assist relay IPs. For perimeter enforcement, push an emergency ACL on the upstream router/firewall denying outbound from the SharePoint server's IP to those destinations.

Evidence: BEFORE isolating the host or blocking outbound connections, capture: (1) full memory dump of the SharePoint server using ProcDump or WinPMEM to preserve in-memory artifacts from w3wp.exe and any injected processes; (2) 'Get-NetTCPConnection -State Established' output with associated PIDs to document active tunnel sessions; (3) 'netstat -ano' timestamped output; (4) running process list via 'Get-Process' and 'tasklist /svc' to correlate cloudflared.exe, code.exe (VS Code tunnel), and ZohoAssist.exe PIDs with parent processes; (5) active network connections including remote IPs for Cloudflare Tunnel (typically *.trycloudflare.com or *.cloudflareaccess.com) and Zoho Assist relay addresses before any firewall rules terminate those sessions.

Step 2: Detection — Do not assume a single threat actor. Assign independent triage threads to each distinct behavioral cluster observed in logs. Query endpoint and network logs for concurrent anomalies: (a) VS Code tunnel process spawning from SharePoint worker processes (w3wp.exe), (b) Cloudflare Tunnel (cloudflared.exe) running on servers where it has no change-managed justification, (c) Zoho Assist remote session initiation outside business hours, (d) DLL sideloading indicators — unexpected DLLs loaded by signed binaries in non-standard paths, (e) vulnerable driver load events in Windows Security event logs (Event ID 7045 for new service installs; correlate with known BYOVD driver hashes from LOLBAS/LOLDrivers lists). Apply NIST AU-6 (Audit Record Review, Analysis, and Reporting) and CIS 8.2 (Collect Audit Logs) to ensure log sources are intact and queryable. Flag any gaps in audit coverage immediately.

NIST Phase: Detection Analysis

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

Controls: NIST AU-6 (Audit Record Review, Analysis, And Reporting), NIST AU-3 (Content Of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with a configuration that captures Event ID 1 (Process Creation) to detect w3wp.exe spawning code.exe, cloudflared.exe, or ZohoAssist.exe; Event ID 7 (Image Load) to catch DLL sideloading by signed binaries loading unexpected DLLs from non-standard paths (e.g., C:\ProgramData, C:\Users\Public); and Event ID 6 (Driver Load) cross-referenced against the LOLDrivers hash list (https://www.loldrivers.io). Use the following PowerShell to query Windows System Event Log for BYOVD driver installs: 'Get-WinEvent -LogName System | Where-Object {$_.Id -eq 7045} | Select-Object TimeCreated, Message | Export-Csv byovd_services.csv'. Run Autoruns (Sysinternals) with VirusTotal integration to surface unsigned or low-reputation DLLs loaded by SharePoint-related binaries. For multi-actor deconfliction, tag each artifact with a cluster label (Actor-A / Actor-B) in a shared spreadsheet before cross-correlating.

Evidence: This step is analytical and does not alter live state, so volatile capture from Step 1 feeds directly into this phase. Additional evidence to collect before any further host actions: (1) IIS/SharePoint ULS logs from the SharePoint server (default path: C:\Program Files\Common Files\microsoft shared\Web Server Extensions\16\LOGS\) for exploit-indicative URI patterns (e.g., abnormal POST requests to /_layouts/, /_vti_bin/, or /sites/ paths that precede w3wp.exe child process spawning); (2) Windows Security Event Log Event ID 4688 (Process Creation with command-line auditing enabled) filtered on parent process w3wp.exe; (3) Windows System Event Log Event ID 7045 (New Service Installed) for BYOVD driver entries — compare hashes against LOLDrivers; (4) Sysmon Event ID 7 (Image Loaded) logs for DLLs loaded from non-standard paths by signed binaries (a hallmark of the unattributed actor's sideloading chain); (5) Prefetch files (C:\Windows\Prefetch\) for cloudflared.exe, code.exe, and ZohoAssist.exe execution history including first-run timestamps to establish actor timelines.

Step 3: Eradication — Apply all current Microsoft patches for on-premises SharePoint as documented in the Microsoft Security Blog advisory (https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting-active

-exploitation-of-on-premises-sharepoint-vulnerabilities/). Remove unauthorized accounts created during the intrusion (audit via T1136.001/T1136.002 indicators). Revoke and rotate all credentials for accounts present on affected SharePoint servers (NIST AC-2, Account Management; D3-CRO, Credential Rotation). Unload and block vulnerable drivers identified in BYOVD activity. Remove unauthorized remote access tooling (VS Code tunnel, cloudflared, Zoho Assist) from servers where no change record exists.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication and Recovery (Eradication phase)

Controls: NIST AC-2 (Account Management), NIST SI-2 (Flaw Remediation) — [not present verbatim in knowledge base; omitted per citation rules], CIS 7.3 (Perform Automated Operating System Patch Management), CIS 7.4 (Perform Automated Application Patch Management), CIS 5.3 (Disable Dormant Accounts)

Compensating: Before patching, snapshot or image the SharePoint server for forensic preservation. To enumerate unauthorized local accounts created by Storm-2603 or the unattributed actor: 'Get-LocalUser | Select-Object Name, Enabled, LastLogon | Export-Csv local_accounts.csv' and 'net localgroup administrators'. For BYOVD driver removal: use 'sc stop ' followed by 'sc delete ', then add the driver's hash to the Windows Defender Vulnerable Driver Blocklist via WDAC policy. Remove sideloaded DLLs identified in Step 2 Sysmon Image Load logs after verifying they are not legitimate system files using 'Get-FileHash' and comparing against known-good baselines from a clean SharePoint installation. For credential rotation without an enterprise PAM tool, use Active Directory Users and Computers to force password resets on all accounts that authenticated to the SharePoint server during the incident window.

Evidence: BEFORE revoking credentials, rotating passwords, removing accounts, unloading drivers, removing tooling, or applying patches — all of which alter live state — capture: (1) complete memory dump of the SharePoint server if not already acquired in Step 1; (2) export of all active SharePoint site collection administrator accounts via 'Get-SPSite | Get-SPWeb | Get-SPUser' (SharePoint Management Shell) to document attacker-added accounts before removal; (3) registry export of HKLM\SYSTEM\CurrentControlSet\Services for BYOVD driver entries before deletion ('reg export HKLM\SYSTEM\CurrentControlSet\Services services_backup.reg'); (4) file system listing with timestamps for all DLLs loaded by the sideloading chain (use 'Get-ChildItem -Path C:\ProgramData,C:\Users\Public -Recurse -Filter *.dll | Select FullName,LastWriteTime,CreationTime' as a starting point); (5) VSS shadow copy enumeration ('vssadmin list shadows') to confirm whether attackers deleted shadow copies — if intact, preserve them before patching; (6) Scheduled Tasks export ('schtasks /query /fo CSV /v > scheduled_tasks.csv') and Services listing ('sc query type= all state= all > services_full.csv') to document persistence mechanisms before eradication.

Step 4: Recovery — Before restoring SharePoint to production, validate: (a) all identified backdoors and sideloaded DLLs are removed, (b) no unauthorized scheduled tasks or services persist (audit via T1543 indicators), (c) endpoint defenses are fully operational and not impaired (T1562.001 reversal confirmed), (d) a fresh credential rotation is complete for all privileged accounts. Monitor post-restoration for re-emergence of tunneling tool processes and new local account creation. Apply NIST AU-9 (Protection of Audit Information) to confirm logs have not been tampered with during recovery. Reference D3-LAM (Local Account Monitoring) for ongoing account surveillance.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST AU-9 (Protection Of Audit Information), NIST AU-11 (Audit Record Retention), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 4.6 (Securely Manage Enterprise Assets and Software)

Compensating: For post-restoration monitoring without EDR, deploy a Sysmon configuration targeting: Event ID 1 (Process Creation) alerting on cloudflared.exe, code.exe (tunnel mode), ZohoAssist.exe, or any executable spawning from the SharePoint application pool identity; Event ID 11 (File Create) in SharePoint's BIN and web root directories for new DLL drops. Schedule a daily PowerShell job to compare current local group membership against the post-eradication baseline: 'net localgroup administrators >> admin_group_audit.txt'. Use Windows Event Forwarding (WEF) — free, built-in — to ship Security and System logs to a central Windows server acting as a log collector, protecting log integrity without a SIEM. Verify Windows Defender real-time protection is active: 'Get-MpComputerStatus | Select AntivirusEnabled, RealTimeProtectionEnabled'.

Evidence: This step restores production state and therefore must be preceded by confirmation that all forensic artifacts have been preserved from prior phases. Specifically verify before returning to production: (1) audit log integrity check — compare current IIS and SharePoint ULS log file hashes against hashes captured during containment to detect tampering (Event ID 1102 in Security Log indicates audit log clearance by attackers; Event ID 104 in System Log for the same); (2) Autoruns output comparison between the eradicated state and a known-clean SharePoint baseline to confirm no residual autostart entries from sideloaded DLLs or cloudflared/ZohoAssist persistence; (3) Windows Defender / AV scan results post-eradication documented and timestamped; (4) Services and Scheduled Tasks exports re-run post-eradication and diff'd against the pre-eradication snapshot from Step 3 to confirm all Storm-2603 and unattributed-actor persistence mechanisms are removed before the server accepts production traffic.

Step 5: Post-Incident — Conduct a structured review of triage methodology. Assess whether your SOC playbooks assume single-actor intrusions and update scoping checklists to require explicit multi-actor hypothesis testing on every significant incident. Implement detection rules that flag behavioral clusters independently rather than correlating all activity to the first identified actor. Review whether BYOVD driver blocks (via Windows Defender Vulnerable Driver Blocklist or equivalent) are current. Map control gaps to NIST AC-6 (Least Privilege) and AC-5 (Separation of Duties) to reduce the blast radius of future SharePoint compromises. Reference D3-CH (Credential Hardening) and D3-MFA (Multi-factor Authentication) for persistent access hardening.

NIST Phase: Post Incident

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

Controls: NIST AC-5 (Separation Of Duties), NIST AC-6 (Least Privilege), NIST AU-2 (Event Logging), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 7.2 (Establish and Maintain a Remediation Process)

Compensating: For teams without an enterprise detection engineering platform, write Sigma rules targeting the specific behavioral clusters from this incident: (1) a rule for w3wp.exe spawning child processes (code.exe, cloudflared.exe, ZohoAssist.exe) as a SharePoint exploitation indicator; (2) a rule for Sysmon Event ID 7 (Image Loaded) where the loaded DLL path is outside System32/SysWOW64/SharePoint install directories and the loading process is a Microsoft-signed binary — the unattributed actor's sideloading pattern. Publish these rules to your internal detection repository. Schedule a quarterly review of the Windows Defender Vulnerable Driver Blocklist (available at https://learn.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-control/microsoft-recommended-driver-block-rules) as a calendar item. Use osquery on SharePoint servers to enforce ongoing least-privilege checks: 'SELECT * FROM logged_in_users' and 'SELECT * FROM startup_items' on a scheduled basis.

Evidence: This phase does not alter live system state and no volatile capture is required. However, the lessons-learned process should reference and formally archive: (1) the full incident timeline reconstructed from IIS logs, Sysmon logs, and Windows Event Logs showing the chronological interleaving of Storm-2603 activity (SharePoint exploitation → VS Code/cloudflared/Zoho Assist deployment) and the unattributed actor's activity (DLL sideloading, BYOVD driver load, custom backdoor execution) — this dual-timeline is the primary evidence that single-actor triage assumptions caused the investigative blind spot; (2) the BYOVD driver hashes and service names from Event ID 7045 entries, submitted to LOLDrivers (https://www.loldrivers.io) if not already listed; (3) the sideloaded DLL samples and their loading-binary relationships, submitted to a malware repository (MalwareBazaar) for community intelligence; (4) a gap analysis documenting which log sources were absent or incomplete during the investigation, mapped to AU-2 (Event Logging) deficiencies for the remediation roadmap.

Detection Guidance

Primary detection focus is on two parallel behavioral clusters, not one. Conflating them will cause both to persist. Specific indicators to hunt:

1. SharePoint exploitation entry: Review IIS logs on SharePoint servers for anomalous POST requests to /_layouts/ or /_vti_bin/ paths from external IPs with no prior session history. Cross-reference with Windows Security Event ID 4688 (process creation) for w3wp.exe spawning cmd.exe, powershell.exe, or mshta.exe.

2. Legitimate tool abuse (Storm-2603): Query for cloudflared.exe, code.exe (VS Code tunnel mode), and Zoho Assist binaries (ZohoAssist.exe, zaservice.exe) on servers where these tools have no documented, change-managed deployment. Network: look for persistent outbound TLS connections to *.trycloudflare.com, *.tunnel.vscode.dev, and Zoho infrastructure from server-class assets.

3. BYOVD defense evasion: Monitor Windows Event ID 7045 for new kernel driver service installs. Cross-reference driver hashes against the LOLDrivers database (loldrivers.io). Alert on any driver load that disables, unloads, or crashes EDR processes.

4. Second actor (DLL sideloading): Detect DLLs loaded by signed Microsoft or vendor binaries from writable user or temp directories. Use Sysmon Event ID 7 (ImageLoad) filtered for signed process + unsigned or untrusted DLL path combinations. Custom backdoors: baseline outbound connection profiles for affected servers and alert on new external destinations, particularly non-standard ports.

5. Account creation: Alert on Windows Security Event IDs 4720 (local account created) and 4728/4732 (account added to security/admin group) on SharePoint servers. Any account creation not traceable to an approved provisioning workflow is a priority alert. Apply NIST AU-2 (Event Logging) and AU-12 (Audit Record Generation) to confirm these event types are being captured. CIS 8.2 (Collect Audit Logs) should be validated as active across all affected systems.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`*.trycloudflare.com`	Cloudflare Tunnel infrastructure used by Storm-2603 for persistent remote access tunneling from compromised SharePoint servers	MEDIUM
DOMAIN	`*.tunnel.vscode.dev`	Visual Studio Code remote tunneling infrastructure used to establish persistent access to compromised environment	MEDIUM
URL	`https://www.microsoft.com/en-us/security/blog/2026/06/22/one-intrusion-two-cyberattackers-uncovering-parallel-threat-activity/`	Primary Microsoft DART incident report — consult for additional IOCs published by Microsoft	HIGH

Framework Mappings

MITRE-ATTACK

- **T1219** — Remote Access Tools
- **T1505.003** — Web Shell
- **T1059** — Command and Scripting Interpreter

- **T1021.004** — SSH
- **T1136.001** — Local Account
- **T1078** — Valid Accounts
- **T1068** — Exploitation for Privilege Escalation
- **T1190** — Exploit Public-Facing Application
- **T1574.002** — DLL Side-Loading
- **T1070** — Indicator Removal
- **T1543** — Create or Modify System Process
- **T1572** — Protocol Tunneling
- **T1562.001** — Disable or Modify Tools
- **T1036** — Masquerading
- **T1136.002** — Domain Account
- **T1078.002** — Domain Accounts

NIST-800-53R5

- **CM-2** — Baseline Configuration
- **CM-7** — Least Functionality
- **SI-3** — Malicious Code Protection
- **SI-4** — System Monitoring
- **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
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **AC-3** — Access Enforcement
- **CP-9** — System Backup
- **IR-4** — Incident Handling

OWASP-TOP10-2021

- **A01:2021** — Broken Access Control

CIS-V8

- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control

- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets

HIPAA-SECURITY

- **164.312(a)(1)** — Access Control
- **164.308(a)(7)(ii)(A)** — Data Backup Plan

NIST-CSF-2

- **RS.MI-01** — Incidents are contained
- **DE.CM-01** — Networks and network services are monitored

ISO-27001-2022

- **A.5.29** — Information security during disruption
- **A.5.23** — Information security for use of cloud services

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1219	Remote Access Tools	Command-And-Control
T1505.003	Web Shell	Persistence
T1059	Command and Scripting Interpreter	Execution
T1021.004	SSH	Lateral-Movement
T1136.001	Local Account	Persistence
T1078	Valid Accounts	Defense-Evasion
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1190	Exploit Public-Facing Application	Initial-Access
T1574.002	DLL Side-Loading	Persistence
T1070	Indicator Removal	Defense-Evasion
T1543	Create or Modify System Process	Persistence
T1572	Protocol Tunneling	Command-And-Control
T1562.001	Disable or Modify Tools	Defense-Evasion
T1036	Masquerading	Defense-Evasion

Technique ID	Technique Name	Tactic
T1136.002	Domain Account	Persistence
T1078.002	Domain Accounts	Defense-Evasion

Sources

Source	URL	Tier
Microsoft Security Blog	https://www.microsoft.com/en-us/security/blog/2026/06/22/one-intrus...	T1
	https://www.microsoft.com/en-us/security/blog/2026/06/22/one-intrus...	T1
Disrupting active exploitation of on-premises SharePoint ... - Microsoft	https://www.microsoft.com/en-us/security/blog/2025/07/22/disrupting...	T1
Cloudflare protects against critical SharePoint vulnerability, CVE ...	https://blog.cloudflare.com/cloudflare-protects-against-critical-sh...	T3
[PDF] Microsoft Incident Response - CYBERATTACK SERIES No. 9	https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/micro...	T1

Generated 2026-06-22 13:57 UTC by TJS Security Command Center