INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-05-12 19:06 UTC

Trusted Third-Party IT Provider Abused as Attack Infrastructure in 123-Day Stealthy Intrusion

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0307
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	HPE Operations Agent (OA), HPE Operations Manager (HPOM), Windows (LSASS, Credential Manager APIs, Network Provider DLLs, LSA Password Filters), Microsoft Defender, Microsoft Defender for Endpoint, Microsoft Defender XDR
Published	2026-05-12T15:00:00+00:00
Discovery Source	Rss:T1 Threatintel

Executive Summary

An unidentified threat actor compromised a trusted third-party IT services provider and used that relationship to maintain undetected access to a target organization for 123 days. The attacker operated exclusively through legitimate HPE Operations Manager management tooling and abused Windows authentication mechanisms to harvest credentials in cleartext, enabling lateral movement to domain controllers. The business risk is severe: this attack exploited the implicit trust, privileged access, and monitoring gaps that third-party IT management relationships typically carry, meaning standard security controls may offer little visibility or resistance.

Technical Analysis

The attacker pivoted through a compromised third-party IT provider that held a delegated management relationship with the victim organization, inheriting associated firewall exceptions, privileged agent accounts, and reduced endpoint monitoring posture. Attack execution relied on HPE Operations Agent (OA) and HPE Operations Manager (HPOM) as the primary command-and-control channel, blending malicious activity into normal IT management traffic. Credential harvesting exploited Windows extensibility without deploying discrete malware by injecting unauthorized DLLs into the authentication stack via two mechanisms: (1) Network Provider DLLs (T1556.002) and (2) LSA Password Filters (T1556), both intercept credentials in cleartext during the Windows authentication sequence. Harvested credentials were used to conduct lateral movement using valid (stolen) accounts (T1078), exploiting the implicit trust of legitimate domain accounts. Lateral movement proceeded via SMB/Windows Admin Shares (T1021.002) and Remote Services (T1021) to domain controllers

and sensitive assets. LSASS was targeted for additional credential access (T1003.001). Persistence was established via boot/logon autostart mechanisms (T1547) and potentially web shells (T1505.003). The attacker also conducted network/system reconnaissance (T1016, T1590, T1591) and account enumeration (T1087.002) before exfiltrating data (T1041). Relevant CWEs: CWE-269 (Improper Privilege Management), CWE-284 (Improper Access Control), CWE-522 (Insufficiently Protected Credentials). No CVE identifier is associated with this campaign. Detection and investigation were performed by Microsoft Defender XDR. No public patch is applicable; this is an abuse of legitimate functionality, not a software vulnerability. Source: Microsoft Security Blog (T1, 2026-05-12).

Action Checklist

1. Containment: Audit all third-party IT provider access immediately - enumerate privileged accounts, agent service accounts, and firewall exceptions granted to managed service providers; suspend or scope-limit any third-party access that cannot be justified by current operational need. Review HPE Operations Agent and HPOM agent accounts for unauthorized configuration changes or lateral use.
2. Detection: Hunt for Network Provider DLL and LSA Password Filter abuse by checking HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order and HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages and PasswordFilters registry keys for unexpected entries; alert on DLL registration changes in these paths. Review Windows Security Event logs for Event ID 4624 (logon) and 4648 (explicit credential use) originating from HPE OA/HPOM service accounts outside of expected maintenance windows. Query Microsoft Defender XDR advanced hunting for LSA-related DLL loads from non-standard paths.
3. Eradication: Remove unauthorized Network Provider DLLs and LSA Password Filter DLLs identified during detection; restore registry keys to known-good baselines. Rotate all credentials that traversed affected systems, prioritizing domain administrator and service accounts. Review and revoke any persistent access tokens or stored credentials associated with the compromised third-party provider.
4. Recovery: Validate domain controller integrity by reviewing AD object modification logs (Event ID 5136, 4662), group membership changes, and new account creation in the 123-day window prior to detection as a reference frame. Re-baseline HPE Operations Manager configuration and agent inventory. Enable Credential Guard on all domain-joined Windows systems where supported to prevent future LSA credential interception. Monitor for re-establishment of unauthorized registry entries post-remediation.
5. Post-Incident: Formalize third-party access governance by implementing just-in-time privileged access for all MSP/IT provider relationships, requiring MFA on all provider-managed accounts, and establishing monitoring parity between internal and third-party management traffic. Map all implicit trust paths (firewall exceptions, agent service accounts, reduced EDR policy scopes) granted to external IT providers and treat them as high-risk attack surface requiring dedicated detection logic. Reference NIST SP 800-161 (Supply Chain Risk Management) and MITRE ATT&CK T1199 (Trusted Relationship) for control framework mapping.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE

Escalation Criteria	Escalate to executive leadership, legal counsel, and breach notification review if any domain administrator credential captured by the LSA Password Filter or Network Provider DLL is confirmed to have authenticated against systems storing PII, PHI, PCI-scoped data, or regulated financial records, or if evidence of AD persistence objects (new accounts, group membership changes, GPO modifications) is identified within the 123-day window — each condition independently triggers regulatory notification assessment under applicable frameworks (GDPR 72-hour window, HIPAA 60-day window, PCI DSS Requirement 12.10).
Recovery Notes	Prior to restoring HPE Operations Manager management connectivity, re-issue all HPOM agent certificates and validate agent-to-server trust using only certificates generated after the confirmed compromise start date; any certificate issued during the 123-day window should be treated as potentially attacker-observed and revoked. Monitor all domain controllers for re-appearance of Event ID 5136 (AD object modification) and re-registration of DLLs in the LSA PasswordFilters and NetworkProvider\Order registry paths for a minimum of 30 days post-remediation using Sysmon Event ID 13 alerts. Given the 123-day dwell time, assume the attacker had sufficient time to establish secondary persistence mechanisms beyond the identified DLLs — conduct a full Autoruns (Sysinternals) sweep across all domain controllers and HPOM-managed hosts and compare output against a known-good baseline before declaring full recovery.
Forensic Artifacts	Malicious LSA Password Filter DLLs and Network Provider DLLs: file path, SHA-256 hash, digital signature status, and creation/modification timestamps — these DLLs are the primary payload for cleartext credential harvesting and are the most specific artifacts of this attack's credential theft mechanism; preserve copies before eradication. | Registry exports of HKLM\SYSTEM\CurrentControlSet\Control\Lsa (PasswordFilters, Authentication Packages) and HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order at time of detection — the attacker's DLL names will appear as unexpected entries and establish when the persistence was installed via registry key LastWriteTime metadata. | HPE HPOM management server policy deployment logs at %OvDataDir%\log\ and HPOM agent logs at %OvAgentDir%\log\ on managed nodes — these logs will show attacker-directed policy deployments used to stage or execute the credential harvesting DLL installation via legitimate HPOM tooling, which is the defining characteristic of this living-off-the-land campaign. | Windows Security Event Log Event ID 4624 (Type 3 network logon) and 4648 (explicit credential use) sourced from HPE OA/HPOM service account SIDs across all domain-joined hosts for the full 123-day window — lateral movement to domain controllers will appear as Type 3 logons from the HPOM service account SID to DC hostnames outside of documented maintenance windows. | Microsoft Defender for Endpoint (MDE) DeviceImageLoadEvents telemetry filtered for DLLs loaded into lsass.exe from non-System32 paths, and any MDE alert suppression or exclusion rules scoped to HPE OA/HPOM processes — the latter will reveal whether the attacker or a misconfigured MSP policy blinded EDR to the DLL injection activity.

Per-Action IR Details

Containment — Audit all third-party IT provider access immediately: enumerate privileged accounts, agent service accounts, and firewall exceptions granted to managed service providers; suspend or scope-limit any third-party access that cannot be justified by current operational need. Review HPE Operations Agent and HPOM agent accounts for unauthorized configuration changes or lateral use.

NIST Phase: Containment

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

Controls: NIST IR-4 (Incident Handling), NIST AC-17 (Remote Access), NIST AC-2 (Account Management), CIS 5.1 (Establish and Maintain an Inventory of Accounts), CIS 6.2 (Establish an Access Revoking Process), CIS 4.4 (Implement and Manage a Firewall on Servers)

Compensating: Run 'net user /domain' and 'Get-ADServiceAccount -Filter *' to enumerate all service accounts; cross-reference against known HPE OA/HPOM service account names (e.g., opc_op, opcuser). Use 'netsh advfirewall firewall show rule name=all' to dump firewall exceptions and grep for MSP IP ranges. Disable non-essential HPE OA agent-to-HPOM server communication via Windows Firewall rule block until investigation concludes: 'netsh advfirewall firewall add rule name="BLOCK_HPOM" dir=in action=block remoteip='.

Evidence: Before suspending any accounts, capture: (1) full output of 'Get-ADUser -Filter * -Properties LastLogonDate,MemberOf' filtered to HPE OA/HPOM service accounts to document last activity and group memberships; (2) Windows Security Event Log Event ID 4728/4732/4756 (group membership additions) for those service accounts over the 123-day window; (3) firewall rule export via 'netsh advfirewall export' to preserve the attack-era exception set; (4) HPE HPOM server-side policy deployment logs at %OvDataDir%\log\ on the HPOM management server showing which nodes received policy pushes and when.

Detection — Hunt for Network Provider DLL and LSA Password Filter abuse: check HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order and HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\Authentication Packages and PasswordFilters registry keys for unexpected entries; alert on DLL registration changes in these paths. Review Windows Security Event logs for Event ID 4624 (logon) and 4648 (explicit credential use) originating from HPE OA/HPOM service accounts outside of expected maintenance windows. Query Microsoft Defender XDR advanced hunting for LSA-related DLL loads from non-standard paths.

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 AU-3 (Content of Audit Records), CIS 8.2 (Collect Audit Logs)

Compensating: Deploy Sysmon with SwiftOnSecurity config (minimum): Sysmon Event ID 13 (RegistryValueSet) will fire on writes to HKLM\SYSTEM\CurrentControlSet\Control\Lsa\PasswordFilters and NetworkProvider\Order. Use this PowerShell one-liner to baseline current DLL registrations: '(Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa").PasswordFilters; (Get-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order").ProviderOrder'. For Event ID 4624/4648 hunting without SIEM, run: 'Get-WinEvent -LogName Security | Where-Object {$_.Id -in @(4624,4648) -and $_.Message -match "opcuser|opc_op|"}'. For DLL path validation, use Sigcheck (Sysinternals) on each registered DLL: 'sigcheck -accepteula -e -u ' to identify unsigned or untrusted binaries.

Evidence: Capture before any registry remediation: (1) full registry export of HKLM\SYSTEM\CurrentControlSet\Control\Lsa and HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider via 'reg export HKLM\SYSTEM\CurrentControlSet\Control\Lsa lsa_export.reg'; (2) file metadata (creation time, hash, signer) of every DLL listed in PasswordFilters and NetworkProvider\Order using 'Get-FileHash' and 'Get-AuthenticodeSignature'; (3) Windows Security Event Log filtered for Event ID 4624 Type 3 (network logon) and 4648 sourced from HPOM service account SIDs over the full 123-day window; (4) Sysmon Event ID 7 (ImageLoaded) logs if Sysmon was deployed, filtered for DLLs loaded into lsass.exe from non-System32 paths; (5) Microsoft Defender XDR Advanced Hunting query: DeviceImageLoadEvents | where InitiatingProcessFileName =~ 'lsass.exe' | where not(FolderPath startswith 'C:\\Windows\\System32').

Eradication — Remove unauthorized Network Provider DLLs and LSA Password Filter DLLs identified during detection; restore registry keys to known-good baselines. Rotate all credentials that traversed affected systems, prioritizing domain administrator and service accounts. Review and revoke any persistent access tokens or stored credentials associated with the compromised third-party provider.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

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 5.2 (Use Unique Passwords), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: Before removing any DLL, copy it to a write-protected forensic share for later analysis. Remove registry entries via: 'reg delete "HKLM\SYSTEM\CurrentControlSet\Control\Lsa" /v PasswordFilters /f' followed by re-add with known-good value. Verify DLL file deletion with 'del /f' and confirm removal with Autoruns (Sysinternals) — re-run Autoruns after reboot to confirm persistence is cleared. For credential rotation without enterprise tooling, use 'Set-ADAccountPassword' in a scripted loop against all accounts that authenticated through HPOM-managed hosts; prioritize krbtgt (reset twice, 10 hours apart per Microsoft guidance), domain admin accounts, and all HPE OA/HPOM service accounts. Use 'klist purge' on each affected host to flush cached Kerberos tickets.

Evidence: Before removing any artifact: (1) create a forensic memory image of at least one affected system using WinPmem or DumpIt to preserve in-memory credential material and loaded DLL state in lsass; (2) hash and archive all malicious DLLs with chain-of-custody documentation before deletion — these are primary evidence of the credential harvesting mechanism; (3) export Windows Credential Manager contents via 'cmdkey /list' and document all stored credentials for affected service accounts before rotation; (4) capture 'klist' output on affected hosts to document active Kerberos tickets and their service principal names before purging; (5) export HPOM agent configuration files from %OvAgentDir%\conf\ to document any attacker-modified policy or certificate configurations.

Recovery — Validate domain controller integrity: review AD object modification logs (Event ID 5136, 4662), group membership changes, and new account creation in the 123-day window prior to detection as a reference frame. Re-baseline HPE Operations Manager configuration and agent inventory. Enable Credential Guard on all domain-joined Windows systems where supported to prevent future LSA credential interception. Monitor for re-establishment of unauthorized registry entries post-remediation.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST SI-6 (Security and Privacy Function Verification), NIST SI-7 (Software, Firmware, and Information Integrity), NIST CM-2 (Baseline Configuration), NIST AU-11 (Audit Record Retention), CIS 4.6 (Securely Manage Enterprise Assets and Software), CIS 7.1 (Establish and Maintain a Vulnerability Management Process)

Compensating: Query AD modification events without SIEM using: 'Get-WinEvent -ComputerName -LogName "Security" | Where-Object {$_.Id -in @(5136,4662,4720,4728)} | Where-Object {$_.TimeCreated -gt (Get-Date).AddDays(-123)}'. For Credential Guard enablement, use Group Policy: Computer Configuration > Administrative Templates > System > Device Guard > Turn On Virtualization Based Security — set to Enabled with Credential Guard set to 'Enabled with UEFI lock'. Validate Credential Guard is active post-reboot with: '(Get-WmiObject -ClassName Win32_DeviceGuard -Namespace root\Microsoft\Windows\DeviceGuard).SecurityServicesRunning' (value 1 = Credential Guard running). For HPE OA re-baselining, compare current agent configuration against the HPOM server's trusted policy store and revoke/re-issue any agent certificates that were active during the 123-day compromise window.

Evidence: Before declaring recovery complete: (1) pull Domain Controller Security Event Log for Event ID 5136 (directory service object modification) and 4720 (user account created) scoped to the 123-day intrusion window — this is the primary record of any AD persistence the attacker may have established; (2) run 'Get-ADObject -Filter {WhenCreated -gt (Get-Date).AddDays(-123)} -Properties *' to identify all AD objects created during the compromise window; (3) collect HPE HPOM policy audit logs from the management server to identify which agent nodes received configuration pushes and whether any rogue policies were deployed; (4) run 'reg query HKLM\SYSTEM\CurrentControlSet\Control\Lsa' and 'HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order' on all domain-joined hosts post-remediation to verify no re-registration of malicious DLLs; (5) verify krbtgt password reset completion by checking Event ID 4723/4724 on the PDC emulator.

Post-Incident — Formalize third-party access governance: implement just-in-time privileged access for all MSP/IT provider relationships, require MFA on all provider-managed accounts, and establish monitoring parity between internal and third-party management traffic. Map all implicit trust paths (firewall exceptions, agent service accounts, reduced EDR policy scopes) granted to external IT providers and treat them as high-risk attack surface requiring dedicated detection logic. Reference NIST SP 800-161 (Supply Chain Risk

Management) and MITRE ATT&CK T1199 (Trusted Relationship) for control framework mapping.

NIST Phase: Post Incident

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

Controls: NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), NIST IR-6 (Incident Reporting), NIST SA-9 (External System Services), NIST AC-2 (Account Management), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access), CIS 5.1 (Establish and Maintain an Inventory of Accounts)

Compensating: Document all implicit trust paths in a spreadsheet: columns for provider name, account name, SID, firewall rule name/port, EDR exclusion scope, and business justification — treat any row without a current justification as an immediate revocation candidate. For JIT access without a PAM platform, implement a manual ticketed procedure: MSP access requires a same-day ServiceNow (or equivalent) ticket with approval, followed by temporary firewall rule activation via 'netsh advfirewall' and automatic expiry via a scheduled PowerShell task that re-blocks the rule after the maintenance window. Write a Sigma rule targeting Sysmon Event ID 13 on HKLM\SYSTEM\CurrentControlSet\Control\Lsa\PasswordFilters and HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order to provide ongoing detection of the specific persistence mechanism used in this campaign — map it to MITRE ATT&CK T1556.002 (Modify Authentication Process: Password Filter DLL) and T1199 (Trusted Relationship).

Evidence: For the post-incident review: (1) compile the complete timeline of HPOM management server connections to the target environment over the 123-day window from firewall flow logs and Windows Security Event ID 4624 Type 3 logs — this reconstructs the attacker's operational pattern and validates dwell time claims; (2) collect all Microsoft Defender for Endpoint alert suppression rules and exclusion configurations that were active during the intrusion period to document whether EDR telemetry was degraded for HPOM-associated processes; (3) document the full list of accounts whose credentials were exposed to the malicious LSA Password Filter and Network Provider DLLs — this list defines the mandatory credential rotation scope and informs breach notification decisions.

Detection Guidance

Primary detection focus is registry-based LSA extensibility abuse and anomalous use of HPE management tooling. (1) Registry monitoring: alert on any write to HKLM\SYSTEM\CurrentControlSet\Control\Lsa\PasswordFilters or HKLM\SYSTEM\CurrentControlSet\Control\NetworkProvider\Order; these keys should change rarely and only during approved software installation. Use Sysmon Event ID 13 (RegistryValueSet) or Microsoft Defender for Endpoint registry alerts. (2) DLL load monitoring: flag DLL loads into LSASS from non-standard or recently created paths using Sysmon Event ID 7 (ImageLoaded) filtered on TargetImage containing lsass.exe. (3) HPE tooling misuse: baseline normal HPE Operations Agent execution patterns; alert on HPE OA/HPOM processes spawning unexpected child processes, executing PowerShell, or accessing credential stores outside of maintenance windows. (4) Credential use anomalies: correlate Event ID 4624 Type 3 (network logon) and 4648 (explicit credentials) from HPE service accounts against approved change windows; lateral movement to domain controllers from these accounts outside approved windows is a high-fidelity indicator. (5) LSASS access: alert on non-system processes opening LSASS with PROCESS_VM_READ access (Sysmon Event ID 10, TargetImage lsass.exe). Microsoft's LSASS credential dumping detection guidance (Microsoft Security Blog, 2022-10-05) provides additional rule templates. Microsoft did not publish IOCs (IPs, domains, file hashes) in the public advisory for this campaign, limiting external hunt capability. Organizations should focus on behavioral detection as outlined above.

Framework Mappings

MITRE-ATTACK

- **T1556.002** — Password Filter DLL
- **T1078** — Valid Accounts
- **T1547** — Boot or Logon Autostart Execution
- **T1556** — Modify Authentication Process
- **T1590** — Gather Victim Network Information
- **T1003.001** — LSASS Memory
- **T1591** — Gather Victim Org Information
- **T1021** — Remote Services
- **T1003** — OS Credential Dumping
- **T1068** — Exploitation for Privilege Escalation
- **T1021.002** — SMB/Windows Admin Shares
- **T1574** — Hijack Execution Flow
- **T1016** — System Network Configuration Discovery
- **T1505.003** — Web Shell
- **T1199** — Trusted Relationship
- **T1087.002** — Domain Account
- **T1041** — Exfiltration Over C2 Channel

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
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-17** — Remote Access
- **AC-3** — Access Enforcement
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **CM-2** — Baseline Configuration
- **CA-7** — Continuous Monitoring
- **SI-16** — Memory Protection
- **SI-10** — Information Input Validation
- **SR-2** — Supply Chain Risk Management Plan

OWASP-TOP10-2021

- **A03:2021** — Injection

- **A01:2021** — Broken Access Control
- **A04:2021** — Insecure Design
- **A07:2021** — Identification and Authentication Failures

CIS-V8

- **16.10** — Apply Secure Design Principles in Application Architectures
- **5.4** — Restrict Administrator Privileges to Dedicated Administrator Accounts
- **6.8** — Define and Maintain Role-Based Access Control
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **5.2** — Use Unique Passwords
- **6.3** — Require MFA for Externally-Exposed Applications
- **15.1** — Establish and Maintain an Inventory of Service Providers
- **8.2** — Collect Audit Logs

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(a)(1)** — Access Control
- **164.308(a)(5)(ii)(D)** — Password Management
- **164.312(d)** — Person or Entity Authentication

NIST-CSF-2

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

ISO-27001-2022

- **A.5.21** — Managing information security in the ICT supply chain

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1556.002	Password Filter DLL	Credential-Access
T1078	Valid Accounts	Defense-Evasion
T1547	Boot or Logon Autostart Execution	Persistence
T1556	Modify Authentication Process	Credential-Access
T1590	Gather Victim Network Information	Reconnaissance

Technique ID	Technique Name	Tactic
T1003.001	LSASS Memory	Credential-Access
T1591	Gather Victim Org Information	Reconnaissance
T1021	Remote Services	Lateral-Movement
T1003	OS Credential Dumping	Credential-Access
T1068	Exploitation for Privilege Escalation	Privilege-Escalation
T1021.002	SMB/Windows Admin Shares	Lateral-Movement
T1574	Hijack Execution Flow	Persistence
T1016	System Network Configuration Discovery	Discovery
T1505.003	Web Shell	Persistence
T1199	Trusted Relationship	Initial-Access
T1087.002	Domain Account	Discovery
T1041	Exfiltration Over C2 Channel	Exfiltration

Sources

Source	URL	Tier
Microsoft Security Blog	https://www.microsoft.com/en-us/security/blog/2026/05/12/underminin...	T1
	https://www.microsoft.com/en-us/security/blog/2026/05/12/underminin...	T1
	https://www.microsoft.com/en-us/security/blog/2026/05/01/cve-2026-3...	T1
MS Defender for Endpoint for Servers - Attack Surf... - HPE Community	https://community.hpe.com/t5/servers-general/ms-defender-for-endpoi...	T3
Detecting and preventing LSASS credential dumping attacks	https://www.microsoft.com/en-us/security/blog/2022/10/05/detecting-...	T1

Generated 2026-05-12 19:06 UTC by TJS Security Command Center