INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-04-01 06:05 UTC

Mass Wipe Campaign Exploits Microsoft Entra ID and Intune; CISA Operational Capacity Degraded

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.1

SCC Item ID	SCC-CAM-2026-0133
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.1
Affected Products	Microsoft Entra ID (all tenants), Microsoft Intune (all tenants), Stryker Corporation, U.S. government organizations, organizations across 79 countries
Published	2026-03-30
Discovery Source	Gemini

Executive Summary

An unattributed threat actor compromised Microsoft Entra ID credentials to gain authenticated access to Microsoft Intune, then used Intune's native device wipe functionality to destroy more than 200,000 systems across 79 countries while exfiltrating approximately 50 terabytes of data. Stryker Corporation is a confirmed victim; CISA issued an alert on 2026-03-18 urging all organizations to harden endpoint management systems. The attack exploited no software vulnerability, it abused legitimate administrative tooling, meaning organizations without strong identity controls and Intune audit monitoring face the same exposure today.

Technical Analysis

Attack vector: credential compromise of Microsoft Entra ID accounts with delegated Microsoft Intune administrative rights, followed by abuse of Intune's legitimate MDM wipe commands (T1078.004, Cloud Accounts, T1078, Valid Accounts). No CVE is assigned; the attack chain relies on stolen or phished credentials rather than a software flaw. Relevant weaknesses: CWE-522 (Insufficiently Protected Credentials), CWE-284 (Improper Access Control), CWE-778 (Insufficient Logging). Post-authentication activity mapped to T1485 (Data Destruction), T1486 (Data Encrypted for Impact, wipe analog), T1530 (Data from Cloud Storage). Approximately 50 TB of data was exfiltrated prior to the destructive wipe phase. No patch is available or applicable, remediation is entirely control-based: conditional access policy enforcement, Intune RBAC scoping, privileged identity management, and audit log retention. CISA alert: https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-urges-endpoint-management-system-hardening-after-cyberattack-against-us-organization (T1 source, verify currency at time of use).

Action Checklist

1. Containment, Audit all Entra ID accounts with Intune Device Administrator or Intune Administrator roles immediately. Remove standing privileged access; replace with Privileged Identity Management (PIM) just-in-time activation for all Intune administrative roles. Enforce phishing-resistant MFA (FIDO2 or certificate-based) on all accounts with Intune management rights. Block legacy authentication protocols in Entra ID Conditional Access to eliminate credential stuffing vectors.
2. Detection, Query Entra ID Sign-In Logs and Unified Audit Logs for bulk or off-hours wipe commands: filter Microsoft Intune audit events for 'wipeDevice' and 'deleteDevice' actions, especially from accounts that authenticated from unfamiliar IPs, new ASNs, or outside normal working hours. Review Microsoft Defender for Cloud Apps alerts for impossible travel or atypical token usage on Intune-privileged accounts. Alert on any single account initiating wipe actions against more than 5 devices within a 1-hour window.
3. Eradication, Rotate credentials for all Entra ID accounts with Intune administrative rights. Revoke and reissue all active sessions and refresh tokens for those accounts (use Entra ID 'Revoke Sign-In Sessions'). Scope Intune RBAC roles to least privilege: separate device enrollment, device configuration, and device wipe permissions across distinct role assignments. Enforce Conditional Access policies requiring compliant devices and named locations for Intune administrative actions.
4. Recovery, Validate that PIM activation logging is active and alerting on all Intune privileged role activations. Confirm Intune audit logs are retained for a minimum of 90 days and are forwarded to your SIEM. Re-inventory all managed endpoints to identify any devices with stale enrollment status that may indicate prior wipe actions. Restore affected systems from verified, pre-incident backups; validate backup integrity before restoration.
5. Post-Incident, This attack exposed three control gaps: (1) standing privileged access to destructive administrative functions without JIT controls, (2) absence of anomaly detection on MDM wipe commands at scale, and (3) insufficient credential protection for cloud-privileged accounts. Map findings to NIST SP 800-53 controls AC-6 (Least Privilege), IA-5 (Authenticator Management), and AU-12 (Audit Record Generation). Review CIS Benchmark for Microsoft 365 (Level 2) for Intune and Entra ID hardening guidance. Note: CISA's reduced operational staffing means organizations should not rely on timely federal threat notifications; internal detection coverage for this attack pattern is essential.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate immediately to legal counsel and executive leadership if Intune wipe audit logs confirm any managed devices contained PHI, PII, or data subject to GDPR, HIPAA, or state breach notification laws, or if device count exceeds organizational incident severity thresholds; additionally escalate if CISA KEV or sector-specific ISAC intelligence confirms the same threat actor is actively targeting your industry vertical.

Recovery Notes	Re-enrollment of wiped endpoints must not proceed until Entra ID token revocation and PIM JIT controls are confirmed active — restoring devices to an environment where the threat actor retains valid session tokens reintroduces the attack surface immediately. Monitor Intune audit logs daily for 30 days post-recovery for any recurrence of bulk wipe commands or anomalous RBAC role activations, as this campaign's use of legitimate administrative APIs means traditional endpoint AV and EDR will not generate alerts on the attack action itself. Given CISA's acknowledged reduced operational capacity as of the 2026-03-18 advisory, do not expect external notification if a follow-on wave targets your tenant — internal detection via the wipe-volume threshold query is the primary safeguard.
Forensic Artifacts	Microsoft Intune Audit Logs (Intune portal > Tenant Administration > Audit Logs): primary record of 'wipeDevice' and 'deleteDevice' actions — each entry contains the initiating account UPN, source IP, target device ID, device name, OS platform, and exact UTC timestamp; this is the definitive evidence of scope and attribution for the wipe campaign. | Entra ID Sign-In Logs for Intune-privileged accounts: captures authentication IP, ASN, device compliance state, MFA method used, token issuance policy, and Conditional Access policy outcome for each session that preceded a wipe action — establishes whether credential stuffing, token theft, or phishing was the initial access vector. | Entra ID Audit Logs filtered on 'Category: RoleManagement' and 'Activity: Add member to role': reveals when the threat actor account was granted Intune Administrator or Intune Device Administrator role membership, establishing the privilege escalation timeline relative to the first wipe command. | Entra ID PIM Activation Logs (Entra ID > Privileged Identity Management > Azure AD Roles > Resource Audit): if PIM was in use pre-incident, these logs show whether JIT activations occurred for Intune roles and whether activation approvals were bypassed — absence of PIM activation records alongside wipe commands confirms standing access was exploited. | Microsoft 365 Unified Audit Log entries for 'RecordType: AzureActiveDirectory' and 'Operations: Add app role assignment to service principal': identifies whether the threat actor registered a new OAuth application or service principal to maintain persistent Intune API access independent of the compromised user credential — a persistence mechanism consistent with campaigns abusing Microsoft 365 administrative APIs.

Per-Action IR Details

Containment — Audit all Entra ID accounts with Intune Device Administrator or Intune Administrator roles immediately. Remove standing privileged access; replace with Privileged Identity Management (PIM) just-in-time activation for all Intune administrative roles. Enforce phishing-resistant MFA (FIDO2 or certificate-based) on all accounts with Intune management rights. Block legacy authentication protocols in Entra ID Conditional Access to eliminate credential stuffing vectors.

NIST Phase: Containment

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

Controls: NIST AC-6 (Least Privilege), NIST IA-5 (Authenticator Management), NIST IR-4 (Incident Handling), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts), CIS 6.3 (Require MFA for Externally-Exposed Applications), CIS 6.5 (Require MFA for Administrative Access)

Compensating: Without an enterprise PAM solution, use the Entra ID portal directly: navigate to Entra ID > Roles and Administrators > 'Intune Administrator' and 'Intune Device Administrator' roles, export current assignments via 'Download assignments' CSV, then manually remove standing assignments. Enable PIM via the Microsoft Entra ID P2 trial (90-day free) if not licensed. For legacy auth blocking without a full Conditional Access policy library, run this PowerShell one-liner to enumerate legacy auth sign-ins before blocking: `Get-MgAuditLogSignIn -Filter "clientAppUsed eq 'Exchange ActiveSync' or clientAppUsed eq 'Other clients'" -Top 1000 | Select UserPrincipalName, ClientAppUsed, CreatedDateTime | Export-Csv legacy_auth_signins.csv`. Block legacy auth via Entra ID > Security > Authentication Methods > Legacy Authentication policy.

Evidence: Before removing role assignments, export the full Entra ID role assignment history from Entra ID > Roles and Administrators for the 'Intune Administrator' and 'Intune Device Administrator' roles — capture all current and recently expired assignments with timestamps. Pull Entra ID Sign-In Logs (retained 30 days in portal, longer if forwarded) filtered on the identified privileged accounts: look for sign-ins with 'clientAppUsed' not equal to 'Browser' or 'Mobile Apps and Desktop clients' (legacy auth indicators), and flag any authentications from ASNs associated with VPS providers or Tor exit nodes. Export the Entra ID Conditional Access policy list to document the pre-incident state before any policy changes are made.

Detection — Query Entra ID Sign-In Logs and Unified Audit Logs for bulk or off-hours wipe commands: filter Microsoft Intune audit events for 'wipeDevice' and 'deleteDevice' actions, especially from accounts that authenticated from unfamiliar IPs, new ASNs, or outside normal working hours. Review Microsoft Defender for Cloud Apps alerts for impossible travel or atypical token usage on Intune-privileged accounts. Alert on any single account initiating wipe actions against more than 5 devices within a 1-hour window.

NIST Phase: Detection Analysis

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

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

Compensating: Without Defender for Cloud Apps or a SIEM, query the Microsoft 365 Unified Audit Log directly via PowerShell using the Search-UnifiedAuditLog cmdlet: `Search-UnifiedAuditLog -StartDate (Get-Date).AddDays(-30) -EndDate (Get-Date) -RecordType MicrosoftIntune -Operations 'wipeDevice','deleteDevice' -ResultSize 5000 | Select UserIds, CreationDate, Operations, AuditData | Export-Csv intune_wipe_audit.csv`. Parse the AuditData JSON column for initiating IP address and target device IDs. For anomaly detection without SIEM, use this PowerShell grouping to surface accounts exceeding 5 wipe actions: `Import-Csv intune_wipe_audit.csv | Group-Object UserIds | Where-Object {$_.Count -gt 5} | Select Name, Count`. Run this query daily via Windows Task Scheduler as a compensating detective control.

Evidence: Capture the full Microsoft Intune Audit Log export from Intune portal > Tenant Administration > Audit Logs, filtered on 'Resource type: Device' and 'Activity: Wipe' and 'Delete' for the 90-day retention window before any logs age out — this is the primary forensic record of which account issued wipe commands to which device IDs and at what timestamps. Simultaneously export Entra ID Sign-In Logs for all accounts that appear in the Intune wipe log; cross-reference authentication IP, device compliance state ('isCompliant'), and token type ('tokenIssuancePolicy') for each wipe-issuing session. Preserve the Unified Audit Log entries for 'Add member to role' events in the Intune Administrator and Intune Device Administrator roles for the 90 days preceding the incident to identify when and how the threat actor obtained role membership.

Eradication — Rotate credentials for all Entra ID accounts with Intune administrative rights. Revoke and reissue all active sessions and refresh tokens for those accounts (use Entra ID 'Revoke Sign-In Sessions'). Scope Intune RBAC roles to least privilege: separate device enrollment, device configuration, and device wipe permissions across distinct role assignments. Enforce Conditional Access policies requiring compliant devices and named locations for Intune administrative actions.

NIST Phase: Eradication

Reference: NIST 800-61r3 §3.4 — Eradication

Controls: NIST IA-5 (Authenticator Management), NIST AC-6 (Least Privilege), NIST IR-4 (Incident Handling), NIST CM-6 (Configuration Settings), CIS 5.2 (Use Unique Passwords), CIS 6.2 (Establish an Access Revoking Process)

Compensating: For credential rotation and session revocation without an enterprise PAM tool, use Microsoft Graph PowerShell: `Revoke-MgUserSignInSession -UserId ` for each identified Intune admin account, followed by `Update-MgUser -UserId -PasswordProfile @{ForceChangePasswordNextSignIn=$true; Password=''}`. For RBAC scoping without a dedicated IAM team, export current Intune custom role definitions via Intune portal > Tenant Administration > Roles > export, document each role's permission set, then create separate custom roles for 'Enrollment Only', 'Configuration Only', and 'Wipe-Authorized' by cloning the built-in Intune Administrator role and removing permissions not required. Name locations for Conditional Access can be defined for free in Entra ID using office egress IP ranges.

Evidence: Before revoking sessions, capture a snapshot of all active refresh tokens for Intune admin accounts using: `Get-MgUserAuthenticationMethod -UserId ` to document registered authentication methods (identify any methods added post-compromise, such as newly registered FIDO2 keys or authenticator apps not provisioned by IT). Export Entra ID Audit Logs filtered on 'Category: UserManagement' and 'Activity: Update user' for the incident window to identify whether the threat actor modified account attributes, registered new MFA methods, or changed UPNs to persist access. Preserve Intune RBAC audit logs showing the full history of role assignments and custom role modifications prior to eradication.

Recovery — Validate that PIM activation logging is active and alerting on all Intune privileged role activations. Confirm Intune audit logs are retained for a minimum of 90 days and are forwarded to your SIEM. Re-inventory all managed endpoints to identify any devices with stale enrollment status that may indicate prior wipe actions. Restore affected systems from verified, pre-incident backups; validate backup integrity before restoration.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.5 — Recovery

Controls: NIST IR-4 (Incident Handling), NIST AU-4 (Audit Storage Capacity), NIST AU-11 (Audit Record Retention), NIST SI-7 (Software, Firmware, and Information Integrity), CIS 7.2 (Establish and Maintain a Remediation Process), CIS 8.2 (Collect Audit Logs)

Compensating: Without a SIEM for log forwarding, configure Entra ID Diagnostic Settings (Entra ID > Diagnostic Settings > Add) to forward SignInLogs and AuditLogs to an Azure Storage Account (lowest-cost archival option) for 90-day retention — estimated cost under $5/month for most tenants. For endpoint re-inventory without enterprise MDM reporting tooling, export the full Intune managed device list via: `Get-MgDeviceManagementManagedDevice -All | Select DeviceName, EnrollmentState, LastSyncDateTime, ComplianceState, OperatingSystem | Export-Csv intune_device_inventory.csv` — devices with EnrollmentState 'unknown' or LastSyncDateTime older than 14 days warrant manual investigation as potential wipe victims. For backup integrity validation without enterprise backup tooling, boot candidate restore images in an isolated VM and verify OS and application hash against known-good baselines using CertUtil: `CertUtil -hashfile SHA256`.

Evidence: Before restoring any wiped endpoints, confirm from Intune audit logs that each device's wipe command was issued by the compromised account (not a legitimate admin action) by correlating device IDs in the wipe log against your pre-incident device inventory — this prevents restoring systems that were legitimately retired. For each device being restored, document the last successful Intune compliance check timestamp and the last known-good configuration profile assignment as the authoritative pre-wipe state baseline. Capture PIM activation logs from Entra ID > Privileged Identity Management > Azure AD Roles > Resource Audit for the incident window to confirm no legitimate admin activations were interleaved with threat actor activity that could indicate a second compromised account.

Post-Incident — This attack exposed three control gaps: (1) standing privileged access to destructive administrative functions without JIT controls, (2) absence of anomaly detection on MDM wipe commands at scale, and (3) insufficient credential protection for cloud-privileged accounts. Map findings to NIST SP 800-53 controls AC-6 (Least Privilege), IA-5 (Authenticator Management), and AU-12 (Audit Record Generation). Review CIS Benchmark for Microsoft 365 (Level 2) for Intune and Entra ID hardening guidance. Note: CISA's reduced operational staffing means organizations should not rely on timely federal threat notifications; internal detection coverage for this attack pattern is essential.

NIST Phase: Post Incident

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

Controls: NIST AC-6 (Least Privilege), NIST IA-5 (Authenticator Management), NIST AU-12 (Audit Record Generation), NIST IR-4 (Incident Handling), NIST IR-8 (Incident Response Plan), CIS 7.1 (Establish and Maintain a Vulnerability Management Process), CIS 5.4 (Restrict Administrator Privileges to Dedicated Administrator Accounts)

Compensating: For teams without a threat intelligence subscription to monitor future campaigns of this type, configure free alerting via CISA's free advisories RSS feed and Microsoft Security Response Center (MSRC) Security Update Guide API — set up a PowerShell script using Invoke-RestMethod against the MSRC CVRF API (`https://api.msrc.microsoft.com/cvrf/v2.0/updates`) to poll weekly for Entra ID and Intune advisories and email results.

For the AU-12 gap (MDM wipe anomaly detection), deploy the open-source Sigma rule equivalent manually: schedule the wipe audit PowerShell query from the Detection step as a daily Task Scheduler job, compare output row count against a rolling 30-day average, and alert via email if the daily wipe count exceeds 2x the baseline — achievable in under 50 lines of PowerShell with Send-MailMessage.

Evidence: The post-incident evidence package for lessons learned must include: (1) the complete Intune audit log CSV showing the full scope of wipe actions (device count, timestamps, duration of campaign) to quantify blast radius; (2) the Entra ID sign-in log entries showing the first observed authentication from the threat actor's IP/ASN to establish initial access timestamp and dwell time before wipe commands began; (3) a before/after comparison of Intune RBAC role assignments and Conditional Access policy states to document the specific configuration gaps that enabled this attack; (4) documentation of which detection controls (if any) fired during the incident and their latency — this gap analysis directly drives the AU-12 and SI-4 remediation roadmap. Preserve all evidence in write-protected storage for a minimum of 90 days or per your jurisdiction's breach notification retention requirement, whichever is longer.

Detection Guidance

Primary log sources: Entra ID Sign-In Logs, Entra ID Audit Logs, Microsoft Intune Audit Logs, Microsoft Defender for Cloud Apps activity logs. Key behavioral indicators: (1) Intune audit events with operation type 'Wipe' or 'Delete' initiated by a single account against multiple devices in a short window, treat any account wiping more than 5 devices per hour as high-priority alert. (2) Entra ID sign-in events showing successful authentication to Intune from a new ASN, country, or user agent immediately followed by administrative activity, correlate against user's baseline. (3) Token issuance for Intune scopes from accounts that did not complete phishing-resistant MFA. (4) Large outbound data transfers from SharePoint, OneDrive, or Azure Blob Storage prior to wipe events (T1530 pre-staging pattern). SIEM query focus: join Entra ID sign-in events to Intune audit events on AccountId where Intune operation contains 'wipe' and sign-in RiskLevel is not 'none', or where authentication occurred outside conditional access policy scope. No public IOCs (IPs, domains, hashes) have been released by CISA or affiliated sources as of 2026-03-18 (publication date of primary alert).

Indicators of Compromise

Type	Value	Context	Confidence
NOTE	`No IOCs available`	No threat actor-specific indicators (IPs, domains, hashes, URLs) have been publicly released for this campaign as of the source data available (CISA alert 2026-03-18 and associated reporting). Monitor CISA, Microsoft Security Response Center, and relevant ISACs for IOC releases. Do not substitute unverified IOCs.	HIGH

Framework Mappings

MITRE-ATTACK

- **T1078.004** — Cloud Accounts
- **T1078** — Valid Accounts

- **T1486** — Data Encrypted for Impact
- **T1485** — Data Destruction
- **T1530** — Data from Cloud Storage
- **T1190** — Exploit Public-Facing Application

NIST-800-53R5

- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **CA-8** — Penetration Testing
- **RA-5** — Vulnerability Monitoring and Scanning
- **SC-7** — Boundary Protection
- **SI-2** — Flaw Remediation
- **SI-7** — Software, Firmware, and Information Integrity
- **AC-3** — Access Enforcement
- **SI-4** — System Monitoring

OWASP-TOP10-2021

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

CIS-V8

- **5.2** — Use Unique Passwords
- **6.1** — Establish an Access Granting Process
- **6.2** — Establish an Access Revoking Process
- **6.3** — Require MFA for Externally-Exposed Applications
- **8.2** — Collect Audit Logs

HIPAA-SECURITY

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

SOC2-TSC

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

ISO-27001-2022

- **A.8.8** — Management of technical vulnerabilities

NIST-CSF-2

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1078.004	Cloud Accounts	Defense-Evasion
T1078	Valid Accounts	Defense-Evasion
T1486	Data Encrypted for Impact	Impact
T1485	Data Destruction	Impact
T1530	Data from Cloud Storage	Collection
T1190	Exploit Public-Facing Application	Initial-Access

Sources

Source	URL	Tier
CISA Urges Endpoint Management System Hardening After ...	https://www.cisa.gov/news-events/alerts/2026/03/18/cisa-urges-endpo...	T1
Stryker Attack Prompts CISA Warning On Endpoint Management ...	https://www.forbes.com/sites/tonybradley/2026/03/19/stryker-attack-...	T3
CISA Advises U.S. Organziations to Harden Microsoft Intune ...	https://www.hipaajournal.com/cisa-harden-microsoft-intune/	T3
US agency asks companies to secure Microsoft tool after Stryker ...	https://www.reuters.com/business/us-agency-asks-companies-secure-mi...	T2
CISA flags rising threats to endpoint management systems after ...	https://industrialcyber.co/cisa/cisa-flags-rising-threats-to-endpoi...	T3

Generated 2026-04-01 06:05 UTC by TJS Security Command Center