INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:42 UTC

Handala Abuses Microsoft Intune Administrative Access to Wipe 80,000 Stryker Devices

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0047
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Microsoft Intune, Microsoft Entra ID, Stryker Corporation enterprise environment (scale: ~80,000 managed endpoints)
Published	2026-03-21

Executive Summary

On March 11, 2026, the Iranian-linked hacktivist group Handala compromised Stryker Corporation's Microsoft Intune environment using stolen administrative credentials, issuing wipe commands to approximately 80,000 managed endpoints and claiming exfiltration of 50TB of data. No custom malware was used; attackers operated entirely through legitimate Intune management capabilities, making the attack difficult to detect through conventional security tooling. Any organization using cloud-based endpoint management platforms with insufficient controls on privileged access faces equivalent exposure to enterprise-scale data destruction and operational disruption.

Technical Analysis

Handala abused compromised Microsoft Entra ID Global Administrator credentials to gain full control of Stryker's Microsoft Intune tenant. The attack chain involved no custom malware; attackers leveraged native Intune device wipe functionality (T1485) after creating a new privileged account (T1136) and escalating to Global Administrator (T1548). Prior to the wipe, approximately 50TB of data was exfiltrated from cloud storage (T1530). The attackers used valid compromised accounts (T1078, T1078.004) and performed account manipulation to maintain persistence (T1098). Applicable weaknesses: CWE-306 (Missing Authentication for Critical Function), CWE-269 (Improper Privilege Management), CWE-284 (Improper Access Control). No CVE is assigned; this is an abuse-of-legitimate-tooling campaign, not a software vulnerability exploit. CISA issued a follow-on advisory urging hardening of Microsoft Intune and equivalent endpoint management platforms. Patch status is not applicable; remediation is entirely configuration and access-control based.

Action Checklist

1. Step 1, Immediate: Audit all current Global Administrator and Intune Administrator role assignments in Microsoft Entra ID; remove accounts that do not require that level of privilege and verify each remaining assignment is expected and active.
2. Step 2, Immediate: Enforce phishing-resistant MFA (FIDO2, Windows Hello for Business, or certificate-based) on all accounts holding Intune Administrator, Global Administrator, or equivalent roles; conditional access policies should block authentication from non-compliant or unexpected locations.
3. Step 3, Detection: Review Microsoft Entra ID audit logs and Intune audit logs for the past 90 days for unexpected account creations, role assignments, bulk device wipe commands, or sign-ins from unfamiliar IPs or geographies; prioritize events tied to privileged roles.
4. Step 4, Assessment: Inventory all accounts with Intune device management permissions, including service principals and third-party integrations; confirm each has the minimum necessary privilege and that no dormant or orphaned accounts retain administrative access.
5. Step 5, Communication: If anomalous activity is identified, notify internal stakeholders (IR team, legal, leadership) and evaluate reporting obligations; reference CISA's advisory for external guidance language.
6. Step 6, Long-term: Implement Privileged Identity Management (PIM) in Microsoft Entra ID to require just-in-time activation and approval workflows for Global Administrator and Intune Administrator roles; establish alerting for any bulk device action commands issued through Intune.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to external IR firm and legal immediately if evidence confirms credential compromise with bulk device wipe commands executed; this indicates active adversary access and requires forensic chain-of-custody preservation and regulatory notification (HIPAA/GDPR implications if device data includes protected health or personal information).
Recovery Notes	Post-containment: (1) Re-image or factory-reset wiped devices from known-good backups; prioritize clinical/manufacturing devices by business criticality. (2) Restore Intune configuration profiles and app deployments from Intune backup/export (captured before wipe). (3) Conduct user acceptance testing on restored devices before returning to production. (4) Implement the compensating controls and PIM workflow from Step 6 before restoring full-scale Intune device management. (5) Schedule post-incident review within 14 days to identify root cause of credential compromise (phishing, credential reuse, unpatched Entra ID application, etc.).
Forensic Artifacts	Microsoft Entra ID Audit Logs (Directory updates, Role assignments, Sign-in activity) — filter for 180 days prior to incident discovery | Microsoft Intune Device Management Audit Logs (Device actions, Bulk operations, Configuration changes) | Entra ID Sign-in Logs with risk detection (focus on Global Admin, Intune Admin accounts; filter by high-risk sign-ins, impossible travel, unfamiliar locations) | Microsoft Defender for Cloud Apps (if enabled) — Conditional Access Policy audit trails and risky user activity reports | Azure Activity Logs (Resource Group > Activity Log) — all write/delete operations on Intune resources, device management policies, role assignments

Per-Action IR Details

Step 1 — Immediate: Audit all current Global Administrator and Intune Administrator role assignments in Microsoft Entra ID; remove accounts that do not require that level of privilege and verify each remaining assignment is expected and active.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-6 (Least Privilege), CIS 6.1 (Establish and Maintain an Inventory of Administrative Accounts)

Compensating: Use Microsoft Graph PowerShell SDK (free, cross-platform) to export role members: Get-MgDirectoryRole | Get-MgDirectoryRoleMember. Cross-reference against HR records and active employee lists manually. Document each assignment with business justification and approval date. For organizations without Graph access, use Azure CLI: az ad role member list --role-id [role-id].

Evidence: Before removing any account: (1) Export full Entra ID audit logs for the past 180 days filtering on role assignment changes (Sign-in logs, Audit logs category 'Directory updates'). (2) Capture current state: Export role membership roster with assignment dates via Graph/CLI. (3) Screenshot or export conditional access policies tied to privileged roles. (4) Document baseline of expected administrators from HR/IAM systems.

Step 2 — Immediate: Enforce phishing-resistant MFA (FIDO2 or certificate-based) on all accounts holding Intune Administrator, Global Administrator, or equivalent roles; conditional access policies should block authentication from non-compliant or unexpected locations.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Containment)

Controls: NIST 800-53 IA-2 (Authentication), NIST 800-53 IA-4 (Identifier Management), CIS 6.5 (Require Phishing-Resistant MFA)

Compensating: For organizations without Entra ID P2 (conditional access): (1) Manually require FIDO2 registration for all privileged accounts via Entra ID MFA settings (free tier supports basic MFA). (2) Use Azure AD sign-in risk detection alerts (free) to flag logins from new geographies; cross-reference against known admin work locations. (3) Create a manual approval workflow: when a privileged account signs in from a new location, require a callback verification to a known phone number before access is granted. Document all approvals in a spreadsheet for audit.

Evidence: Before enforcing MFA: (1) Capture current MFA enrollment status for all privileged accounts (Entra ID > Users > Multi-factor authentication). (2) Export sign-in logs for privileged accounts over past 90 days to establish baseline of expected geographic locations and times. (3) Document which MFA methods are currently supported in your environment. (4) Screenshot current conditional access policies (if any exist).

Step 3 — Detection: Review Microsoft Entra ID audit logs and Intune audit logs for the past 90 days for unexpected account creations, role assignments, bulk device wipe commands, or sign-ins from unfamiliar IPs or geographies; prioritize events tied to privileged roles.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Detection and Analysis)

Controls: NIST 800-53 AU-2 (Audit Events), NIST 800-53 AU-6 (Audit Review, Analysis, and Reporting), CIS 8.2 (Collect Audit Logs)

Compensating: Organizations without advanced Log Analytics: (1) Export raw Entra ID audit logs via Azure portal (Entra ID > Audit logs) as CSV, filter by 'Directory updates', 'Role assignments', 'Add/Delete User', 'Sign-in activity' categories. (2) For Intune, export Device Management > Device actions audit log as CSV. (3) Use Excel/Google Sheets to manually pivot on: account creation date, role assignment date, bulk wipe command counts, sign-in source IP geolocation (cross-reference IP against MaxMind GeoLite2 free database). (4) Create a simple Python script (open-source): parse CSV, flag IPs outside known office geography using geoip2-db-reader.

Evidence: Before analysis: (1) Preserve unmodified copies of Entra ID audit logs (export immediately to offline storage—do not filter/delete in-place). (2) Export Intune audit logs (Devices > Device actions > Audit logs). (3) Export conditional access sign-in risk data for past 90 days. (4) Document baseline: known admin IP ranges, approved

geographic locations, normal sign-in times. (5) Capture list of all service principals and third-party app registrations with device management permissions.

Step 4 — Assessment: Inventory all accounts with Intune device management permissions, including service principals and third-party integrations; confirm each has the minimum necessary privilege and that no dormant or orphaned accounts retain administrative access.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.1 (Detection and Analysis)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-6 (Least Privilege), CIS 6.1 (Establish and Maintain an Inventory of Administrative Accounts)

Compensating: Organizations without third-party IAM tools: (1) Use Azure AD PowerShell or Microsoft Graph to enumerate all role assignments: Get-AzureADDirectoryRoleMember -RoleObjectId [role-id] | Export-Csv. (2) Export app registrations with device management scopes: Get-AzureADApplication | Where {$_.RequiredResourceAccess -match 'DeviceManagement'}. (3) Cross-reference against current HR/employee list to identify dormant accounts (no login in past 90 days; use Entra ID Sign-in logs). (4) Manually document business justification for each service principal; contact owning team if justification is unclear or outdated.

Evidence: Before assessment: (1) Export current state of all role assignments with timestamps. (2) Capture sign-in history (last login date) for all privileged accounts. (3) Document all active app registrations and service principals with their creation dates and last modified dates. (4) Export list of third-party MDM integrations from Intune (Settings > Tenant Administration). (5) Screenshot all custom role definitions in Intune that grant device wipe/reset permissions.

Step 5 — Communication: If anomalous activity is identified, notify internal stakeholders (IR team, legal, leadership) and evaluate reporting obligations; reference CISA's advisory for external guidance language.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.4 (Post-Incident Activities)

Controls: NIST 800-53 IR-4 (Incident Handling), NIST 800-53 IR-6 (Incident Reporting)

Compensating: Organizations without formal IR governance: (1) Create an incident notification template referencing CISA IR-CERT Playbook (free, open-source) and NIST 800-61 language. (2) Establish a contact list: CISO, General Counsel, CEO/CRO, affected business unit leads, external counsel. (3) Document all communication in a shared log with timestamps, recipients, and content summary to satisfy audit trail requirements. (4) Use CISA's Cyber Incident Reporting for Critical Infrastructure Cybersecurity Act (CIRCIA) framework language for any notification to external parties or regulators.

Evidence: Before notification: (1) Complete initial forensic analysis (Steps 3–4) to quantify scope: number of devices wiped, accounts compromised, data exfiltration indicators. (2) Preserve chain of custody documentation for all forensic evidence. (3) Confirm regulatory reporting obligations based on jurisdiction (GDPR, HIPAA, state breach notification laws if Stryker data includes health records). (4) Draft breach notification letter using CISA template language.

Step 6 — Long-term: Implement Privileged Identity Management (PIM) in Microsoft Entra ID to require just-in-time activation and approval workflows for Global Administrator and Intune Administrator roles; establish alerting for any bulk device action commands issued through Intune.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.3 (Eradication and Recovery)

Controls: NIST 800-53 AC-2 (Account Management), NIST 800-53 AC-6 (Least Privilege), NIST 800-53 AU-12 (Audit Generation), CIS 6.3 (Require MFA for Administrative Access)

Compensating: Organizations without Entra ID P2 license (PIM requires P2): (1) Implement standing privilege model with time-based expiration: use Azure CLI to set role assignment expiration on all privileged accounts (Set-AzureADMSPrivilegedRoleAssignment -ProviderId AzureResources -Schedule -ExpirationDateTime [date]). (2) Create manual approval workflow: require two authorized signers (documented in email/ticketing system) to approve any role elevation for 4+ hours. (3) Use Azure Logic Apps (free tier may apply limits) to trigger email notifications to security team on any device bulk action (query Intune audit logs daily). (4) Establish a weekly privileged account

access review: log all role activations/usage in a shared spreadsheet.

Evidence: Before PIM implementation: (1) Document current privileged role holders and their actual job functions (reconcile with assigned roles). (2) Define approval matrix: who approves PIM activation requests and for which roles. (3) Establish baseline for 'normal' bulk device actions: expected frequency, timing, actor. (4) Export Intune device action audit history to establish thresholds for alerting (e.g., trigger alert if >100 devices wiped in 1 hour).

Detection Guidance

Focus detection on three planes: identity, management, and data. In Microsoft Entra ID audit logs, query for events with category 'RoleManagement' where a Global Administrator or Intune Administrator role was assigned within the last 90 days, flag any assignment not tied to a documented change request. In Intune audit logs, query for 'Wipe' or 'RetireDevice' operations, particularly bulk operations or those initiated outside normal business hours; a single wipe command touching more than a small number of devices in a short window is a high-confidence indicator. In Microsoft Entra ID sign-in logs, look for successful authentications on privileged accounts from IP addresses not associated with known corporate egress points, VPN ranges, or expected geographies. In Microsoft Defender for Cloud Apps or equivalent CASB tooling, alert on large-volume data access or download events in OneDrive, SharePoint, or connected cloud storage. Behavioral indicator: a new account created, immediately assigned a privileged role, and then issuing management-plane commands within a short time window is consistent with the Handala TTPs described in this incident. No confirmed public IOCs (IPs, domains, hashes) have been attributed to this specific campaign at this time; monitor threat intelligence feeds for updates.

Indicators of Compromise

Type	Value	Context	Confidence
URL	`No confirmed IOCs publicly attributed to this campaign at time of writing.`	Handala operated using legitimate administrative credentials and native platform tooling; no malware hashes, C2 domains, or attacker infrastructure have been publicly confirmed as of the source reporting.	LOW

Framework Mappings

MITRE-ATTACK

- **T1098** — Account Manipulation
- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts
- **T1078.004** — Cloud Accounts
- **T1485** — Data Destruction
- **T1059** — Command and Scripting Interpreter
- **T1548** — Abuse Elevation Control Mechanism
- **T1485** — Data Destruction

- **T1136** — Create Account
- **T1098** — Account Manipulation
- **T1530** — Data from Cloud Storage
- **T1078** — Valid Accounts

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-3** — Access Enforcement

OWASP-TOP10-2021

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

CIS-V8

- **6.3**
- **5.4**
- **6.8**
- **6.1**
- **6.2**
- **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
- **164.312(d)** — Person or Entity Authentication

NIST-CSF-2

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

ISO-27001-2022

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

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1098	Account Manipulation	Persistence
T1530	Data from Cloud Storage	Collection
T1078	Valid Accounts	Defense-Evasion
T1078.004	Cloud Accounts	Defense-Evasion
T1485	Data Destruction	Impact
T1059	Command and Scripting Interpreter	Execution
T1548	Abuse Elevation Control Mechanism	Privilege-Escalation
T1136	Create Account	Persistence

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/cisa-warns-businesse...	T3
Stryker attack raises concerns about role of device management tool	https://www.cybersecuritydive.com/news/stryker-attack-device-manage...	T3
CISA Advises U.S. Organziations to Harden Microsoft Intune ...	https://www.hipaajournal.com/cisa-harden-microsoft-intune/	T3
CISA urges US orgs to secure Microsoft Intune systems after Stryker ...	https://www.reddit.com/r/cybersecurity/comments/1rxyoej/cisa_urges_...	T3
CISA Urges Organizations to Secure Microsoft Intune Environments ...	https://cybersecuritynews.com/secure-microsoft-intune-environments/	T3

Generated 2026-03-29 18:42 UTC by TJS Security Command Center