INTELLIGENCE BRIEFING
Security Command Center

TLP:CLEAR
2026-03-29 18:34 UTC

Iranian State Actors (Handala / Homeland Justice) Abuse Telegram as C2 to Deliver Windows Malware and Wiper Payloads

THREAT CAMPAIGN | **CRITICAL** | CVSS 9.5

SCC Item ID	SCC-CAM-2026-0083
Type	Threat Campaign
Severity	CRITICAL
CVSS Base Score	9.5
Affected Products	Windows endpoints (unspecified versions); Microsoft Intune (abused for device management post-compromise); Telegram (abused as C2 channel); Stryker Corporation (confirmed victim, approximately 80,000 devices wiped)
Published	2026-03-23
Discovery Source	Rss

Executive Summary

Iranian state-linked threat actors (Handala, attributed to MOIS; Homeland Justice, attributed to IRGC) are actively using Telegram as command-and-control infrastructure to deliver malware and wiper payloads against journalists, dissidents, and enterprise organizations. The reported impact at Stryker Corporation involved approximately 80,000 devices wiped via abuse of Microsoft Intune for mass device reset, alongside data exfiltration and public leaks. Organizations using Microsoft Intune or with Telegram accessible from managed endpoints face elevated risk of destructive, unrecoverable data loss.

Technical Analysis

Handala and Homeland Justice operators use Telegram's bot API as a C2 channel (MITRE T1071.003, Application Layer Protocol: Web Protocols via legitimate services), consistent with living-off-trusted-services (LOTS) tradecraft designed to blend into normal HTTPS traffic and evade network-layer detection. Initial access vectors include phishing (T1566) and trusted relationship abuse (T1199). Post-compromise, attackers created cloud accounts (T1136.003) and leveraged valid accounts including cloud credentials (T1078, T1078.004) to gain access to Microsoft Intune. Intune was then abused to push wiper payloads (T1485, Data Destruction; T1486, Data Encrypted for Impact) at scale, enabling the reset of approximately 80,000 Stryker devices. Additional techniques observed include data exfiltration over C2 (T1041), exfiltration to web services (T1567), screen capture (T1113), local data collection (T1005), and reconnaissance (T1590). FBI seized four associated domains and issued a flash alert. CISA issued guidance on Microsoft Intune hardening. Relevant CWEs: CWE-269 (Improper Privilege Management), CWE-287 (Improper Authentication), CWE-441 (Unintended Proxy or Intermediary). No CVE is associated with this campaign; the exploitation is primarily procedural and configuration-based rather than vulnerability-driven. No patch resolves this; the risk is architectural and configuration-dependent.

Action Checklist

1. Step 1, Immediate: Audit Microsoft Intune administrative accounts now. Remove any unrecognized accounts, revoke suspicious sessions, and enforce phishing-resistant MFA (FIDO2 or certificate-based) on all Intune admin roles. Refer to CISA guidance on Intune hardening issued following the Stryker incident (consult official CISA alerts for current recommendations).
2. Step 2, Immediate: Review Intune device compliance policies and restrict the ability to perform bulk device wipes or resets to a named, minimal set of break-glass accounts. Require approval workflows or dual-authorization for destructive actions where the platform supports it.
3. Step 3, Detection: Search identity logs (Azure AD / Entra ID sign-in logs) for new cloud account creation (T1136.003), unfamiliar service principal activity, and admin role assignments made outside change-control windows. Flag any Intune bulk-action commands executed in the past 90 days not tied to approved change records.
4. Step 4, Detection: Block or alert on Telegram API endpoints (api.telegram.org) at the network perimeter for managed endpoints where Telegram use is not a business requirement. Review proxy and DNS logs for outbound connections to Telegram infrastructure originating from servers or non-user workstations.
5. Step 5, Assessment: Inventory all accounts with Intune Device Administrator, Intune Administrator, and Global Administrator roles. Confirm each account is human-owned, actively managed, and enrolled in MFA. Remove stale or shared accounts. Confirm conditional access policies restrict Intune console access to compliant, known devices from expected locations.
6. Step 6, Communication: If your organization has not reviewed Intune configuration posture since the Stryker disclosure (March 2026), escalate to CISO and notify the identity/endpoint team leads. Reference the FBI flash alert and CISA guidance as the basis for urgency.
7. Step 7, Long-term: Implement privileged identity management (PIM) for Intune and M365 admin roles, requiring just-in-time elevation with approval. Establish a baseline of expected Intune bulk-action behavior and configure alerts for deviations. Review your trusted-relationship and third-party access inventory (T1199) to ensure vendor accounts are scoped minimally and monitored.

IR / Forensic Enrichment

Triage Priority	IMMEDIATE
Escalation Criteria	Escalate to CISO and external IR firm immediately if any evidence of account compromise, unauthorized role assignment, or bulk device wipe activity is detected during Steps 1–3, or if your organization was part of a Stryker vendor ecosystem (IT service providers, managed service providers, or regional healthcare systems).

Recovery Notes	Post-containment recovery requires restoration of wiped devices from backup (if available; validate backup integrity before restoration), verification of Intune device inventory and compliance status, re-enrollment of wiped devices into Intune with updated security baselines, and a forensic review of admin activity logs to confirm no further unauthorized actions occurred. Document all recovered systems and any data loss in the incident closure report.
Forensic Artifacts	Azure AD / Entra ID sign-in logs (90-day retention, queryable via Azure Portal or PowerShell Get-AuditLog) | Intune audit logs and device action history (admin center Reports > Audit Logs, Graph API /deviceManagement/auditEvents) | Windows Event Log Security 4688 (process creation) and 4720 (account creation) on domain-joined endpoints and on-premises identity systems | Proxy/firewall/DNS logs for outbound connections to api.telegram.org and Telegram IP ranges (149.154.160.0/20, 149.154.164.0/22) over the past 180 days | Microsoft 365 unified audit log (Office 365 admin center > Audit > Search) filtered for administrative actions on Intune, Azure AD, and user accounts

Per-Action IR Details

Step 1 — Immediate: Audit Microsoft Intune administrative accounts now. Remove any unrecognized accounts, revoke suspicious sessions, and enforce phishing-resistant MFA (FIDO2 or certificate-based) on all Intune admin roles. Refer to CISA's Intune hardening guidance issued following the Stryker incident.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.3 (Stopping the Attack)

Controls: NIST AC-2(1) (Account Management — Privileged Access), NIST IA-2(1) (Authentication — MFA), CIS 6.2 (Ensure MFA is Enabled for All Azure Accounts)

Compensating: If no Intune console available, use Azure CLI (`az ad user list --filter "userType eq 'Member'"` and `az role assignment list --scope /subscriptions/{id}`) to export admin accounts; cross-reference against HR records and change-control logs to identify unauthorized entries; document removal in an incident log with timestamp and approver name.

Evidence: Before audit: Export Intune admin role membership via Azure AD Portal (save CSV); capture all sign-in logs for Intune console from the past 90 days (Azure Entra ID sign-in logs, filter by app ID 0ee7b798-893e-46e8-b4b5-4090c7f2cd2d for Intune admin center); screenshare or export MFA enrollment status for all admins; archive any conditional access policies tied to Intune roles.

Step 2 — Immediate: Review Intune device compliance policies and restrict the ability to perform bulk device wipes or resets to a named, minimal set of break-glass accounts. Require approval workflows or dual-authorization for destructive actions where the platform supports it.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.2.1 (Containment Strategy — Segmentation of Privileges)

Controls: NIST AC-3 (Access Control Enforcement), NIST AC-5 (Separation of Duties), CIS 1.2.5 (Ensure MFA is Enabled for All Cloud Accounts with Administrative Privileges)

Compensating: If Intune lacks native approval workflows: create an out-of-band approval process (email or ticket system) requiring signed authorization from two named break-glass admins before any bulk wipe is executed; document each approval with the approver's name, date, time, and justification; store approvals in a read-only shared folder with quarterly audit reviews; implement a manual "hold" period (e.g., 24 hours post-approval before execution) as a detective control.

Evidence: Before policy change: Export current Intune device compliance and reset policies (JSON via Graph API: `GET /deviceManagement/deviceCompliancePolicies`); document all accounts with permission to initiate device actions; capture a baseline of all bulk-action commands executed in the past 180 days (if queryable via Intune audit logs); screenshot the current role-based access control (RBAC) settings for device management.

Step 3 — Detection: Search identity logs (Azure AD / Entra ID sign-in logs) for new cloud account creation (T1136.003), unfamiliar service principal activity, and admin role assignments made outside change-control windows. Flag any Intune bulk-action commands executed in the past 90 days not tied to approved change records.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1.2 (Detection and Analysis — Identifying and Confirming an Incident)

Controls: NIST AU-2 (Audit Events), NIST AU-6 (Audit Review, Analysis, and Reporting), CIS 8.5 (Implement Continuous Log Monitoring and Alerting)

Compensating: Export Azure AD sign-in logs manually via PowerShell: `Get-AuditLog -Filter "CreatedDateTime gt $(Get-Date).AddDays(-90) and Result eq 'Success'" | Where-Object {$_.Operations -match 'Add user'}`. Cross-reference new account creation with change-control tickets (manual spreadsheet review). Search Intune audit logs directly (Intune admin center > Reports > Audit Logs) and filter by Operation = 'Bulk Retire' or 'Reset to Factory Settings'; export results and compare timestamps against approved change windows (via change management system or team calendar).

Evidence: Export Azure AD audit logs (90-day retention minimum): `Get-AuditLog -Filter "CreatedDateTime gt $(Get-Date).AddDays(-90)" | Select-Object CreatedDateTime, UserDisplayName, Activity, ModifiedProperties | Export-Csv`. Export Intune audit events via PowerShell (`Get-IntuneAuditEvent`) or via Graph API. Capture all role assignment change events (filter for role changes in Azure AD audit logs). Document the baseline of expected service principals and their creation dates. Save change-control records (tickets) for the same period as a comparison baseline.

Step 4 — Detection: Block or alert on Telegram API endpoints (api.telegram.org) at the network perimeter for managed endpoints where Telegram use is not a business requirement. Review proxy and DNS logs for outbound connections to Telegram infrastructure originating from servers or non-user workstations.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.1.1 (Detection — Network Monitoring) and §3.2.2 (Containment — Network Segmentation)

Controls: NIST SC-7(5) (Boundary Protection — Deny by Default and Allow by Exception), CIS 13.1 (Maintain and Enforce Network-Based URL Filters)

Compensating: If no proxy/firewall available: configure host-based egress rules on Windows endpoints using Windows Defender Firewall (`netsh advfirewall add rule name='Block Telegram API' dir=out action=block remoteip=149.154.160.0/20,149.154.164.0/22 remoteport=443 protocol=tcp`); on non-enterprise networks, block api.telegram.org via DNS sinkhole (Pi-hole or Unbound) by adding it to a blocklist; monitor DNS queries for *.telegram.org via DNS log exports (Windows DNS server or router logs) and cross-reference against user/device inventory quarterly.

Evidence: Before implementing block: Export 90-day proxy/firewall logs filtered for api.telegram.org, telegram.org, or Telegram IP ranges (149.154.160.0/20, 149.154.164.0/22); document source IPs, user accounts, timestamps, and request frequency; capture DNS query logs for *.telegram.org; if available, export Web Data Loss Prevention (DLP) logs from any email/web gateway to identify Telegram file transfers or credential sharing. Save baseline to compare post-remediation.

Step 5 — Assessment: Inventory all accounts with Intune Device Administrator, Intune Administrator, and Global Administrator roles. Confirm each account is human-owned, actively managed, and enrolled in MFA. Remove stale or shared accounts. Confirm conditional access policies restrict Intune console access to compliant, known devices from expected locations.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §2.3 (Preparation — Configuration Management) and NIST 800-53r5 AC-2 (Account Management)

Controls: NIST AC-2(1) (Account Management — Privileged Access), NIST IA-4 (Identifier Management), CIS 6.1 (Ensure Multifactor Authentication (MFA) is Enabled for All Azure Users)

Compensating: Use PowerShell to enumerate privileged roles without Graph API: `Get-MsolRoleMember -RoleObjectId $(Get-MsolRole -RoleName 'Intune Administrator').ObjectId | Select-Object DisplayName, EmailAddress`. Cross-reference against your HR system (manual review or exported CSV) to confirm human ownership; for each account, use `Get-MsolUser -UserPrincipalName | Select-Object *Mfa*` to verify MFA enrollment. Document findings in a spreadsheet; escalate stale accounts (last login >90 days) and shared accounts (no assigned user) for removal. Conditional access policies: if unavailable, implement manual allowlist controls (document approved admin IP ranges and device identifiers; audit sign-in logs monthly).

Evidence: Export role membership via Azure AD Portal (CSV) or PowerShell; capture MFA enrollment status for each admin (export via `Get-MsolUser` or Azure Portal screenshot); document conditional access policies applied to Intune roles (export via Graph API: `GET /identity/conditionalAccess/policies`); save HR/employee roster for cross-reference; export sign-in logs for all privileged accounts over the past 180 days to confirm activity patterns; document any service principals with Intune admin roles and their usage baseline (API call frequency, IP ranges, time-of-day patterns).

Step 6 — Communication: If your organization has not reviewed Intune configuration posture since the Stryker disclosure (approximately March 2026), escalate to CISO and notify the identity/endpoint team leads. Reference the FBI flash alert and CISA guidance as the basis for urgency.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (Preparation — Tools and Resources) and §3.4 (Post-Incident Activity — Lessons Learned)

Controls: NIST IR-1 (Incident Response Policy), NIST IR-2 (Incident Response Training), CIS 19.1 (Establish an Incident Response Team)

Compensating: If no formal escalation process exists: send a written summary (email or memo) to the highest-ranking technical and business stakeholders (CTO, VP of Security, VP of Operations) documenting the threat context, your current Intune configuration exposure (based on Steps 1–5), and the Stryker impact (80,000 devices wiped); include a link to the FBI/CISA advisories; request a meeting within 48 hours to align on remediation timeline; document the escalation with timestamp and recipient list for incident records.

Evidence: Gather FBI flash alert (if available internally; otherwise cite the public notice); save CISA guidance URL and publication date; prepare a 1-page summary of your current Intune admin account posture and any findings from Steps 1–5 that indicate risk; document the date of your last Intune security review (if any) to establish the time gap since Stryker disclosure.

Step 7 — Long-term: Implement privileged identity management (PIM) for Intune and M365 admin roles, requiring just-in-time elevation with approval. Establish a baseline of expected Intune bulk-action behavior and configure alerts for deviations. Review your trusted-relationship and third-party access inventory (T1199) to ensure vendor accounts are scoped minimally and monitored.

NIST Phase: Recovery

Reference: NIST 800-61r3 §3.4.1 (Post-Incident Activity — Lessons Learned) and NIST 800-53r5 AC-6 (Least Privilege)

Controls: NIST AC-6(2) (Least Privilege — Non-Privileged Access for Non-Administrative Tasks), NIST AC-3(7) (Access Control — Role-Based Access Control), CIS 5.2 (Ensure that Multi-Tenant Organization is Configured in Microsoft 365)

Compensating: If PIM (Azure AD P2) is unavailable: implement a manual just-in-time elevation process: create break-glass admin accounts (separate from routine admin accounts) with standing elevated privileges; require all routine Intune administrative tasks to be performed by non-admin accounts; establish an approval workflow (email chain with two-person sign-off) for elevation requests; document each elevation with business justification and duration; audit elevation requests monthly. For behavior baselining: export Intune audit logs monthly and identify the count, timing, and user of bulk-action commands; set a threshold (e.g., more than 5 bulk wipes per day triggers an alert) and implement manual weekly reviews against that threshold.

Evidence: Document current Intune admin accounts and their privileges (baseline from Step 5); establish a baseline of expected bulk-action frequency by querying historical Intune audit logs for the past 6 months (if available); inventory all third-party and vendor accounts with access to Intune or M365 (manual spreadsheet or identity governance system export); capture the creation date, last login date, and scope of access for each vendor account; document the business justification for each vendor account and the point of contact for access reviews.

Detection Guidance

Focus detection on three planes: identity, Intune activity, and network. Identity: Query Entra ID (Azure AD) audit logs for new account creation events (operationName: 'Add user'), role assignments to Intune or Global Admin roles, and MFA registration events for accounts not in your provisioning workflow. Filter for accounts created outside business hours or from unfamiliar IP ranges. Intune: Review Intune audit logs (in Microsoft Endpoint Manager admin center under Tenant Administration > Audit Logs) for bulk device wipe or retire commands, especially those executed by accounts not associated with your endpoint team. Alert on any 'Wipe' or 'Retire' action affecting more than a threshold number of devices in a single session. Network: Alert on outbound HTTPS to api.telegram.org from endpoints where Telegram is not an approved application, particularly servers, CI/CD systems, or administrative workstations. Behavioral indicators consistent with this campaign: admin accounts logging in from new countries or ASNs, service principals accessing Intune Graph API endpoints without a corresponding change ticket, and large volumes of device compliance state changes in a short window. Cross-reference any identified accounts or IPs against indicators released by the FBI (consult official FBI Cyber Division advisories for current IOC lists).

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	`api.telegram.org`	Telegram Bot API endpoint abused as C2 channel by Handala operators (T1071.003). Legitimate domain weaponized for LOTS tradecraft; flagging should be context-aware (non-user endpoints, servers, admin workstations).	MEDIUM
DOMAIN	`[FBI-seized domains — specific values not confirmed in available sources]`	FBI seized four domains associated with this campaign per the flash alert. Specific domain values were not reproduced in the secondary sources available for this item. Obtain the current IOC list directly from the FBI flash alert or CISA advisory.	LOW

Framework Mappings

MITRE-ATTACK

- **T1485** — Data Destruction
- **T1567** — Exfiltration Over Web Service
- **T1486** — Data Encrypted for Impact
- **T1078** — Valid Accounts

- **T1136.003** — Cloud Account
- **T1199** — Trusted Relationship
- **T1583.001** — Domains
- **T1041** — Exfiltration Over C2 Channel
- **T1590** — Gather Victim Network Information
- **T1588.005** — Exploits
- **T1566** — Phishing
- **T1071.003** — Mail Protocols
- **T1005** — Data from Local System
- **T1113** — Screen Capture
- **T1078.004** — Cloud Accounts

NIST-800-53R5

- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution
- **AC-2** — Account Management
- **AC-6** — Least Privilege
- **IA-2** — Identification and Authentication (Organizational Users)
- **IA-5** — Authenticator Management
- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **AT-2** — Literacy Training and Awareness
- **SI-3** — Malicious Code Protection
- **SI-8** — Spam Protection
- **IA-8** — Identification and Authentication (Non-Organizational Users)

OWASP-TOP10-2021

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

CIS-V8

- **5.4**
- **6.8**
- **6.3**
- **6.4**
- **6.5**
- **8.2** — Collect Audit Logs

SOC2-TSC

- **CC6.1** — The entity implements logical access security software, infrastructure, and architectures over protected information assets
- **CC7.4** — Responds to identified security incidents

HIPAA-SECURITY

- **164.312(d)** — Person or Entity Authentication
- **164.308(a)(6)(ii)** — Response and Reporting

ISO-27001-2022

- **A.5.34** — Privacy and protection of personal information

NIST-CSF-2

- **RS.CO-03** — Recovery activities and progress communicated
- **DE.CM-01** — Networks and network services are monitored

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1485	Data Destruction	Impact
T1567	Exfiltration Over Web Service	Exfiltration
T1486	Data Encrypted for Impact	Impact
T1078	Valid Accounts	Defense-Evasion
T1136.003	Cloud Account	Persistence
T1199	Trusted Relationship	Initial-Access
T1583.001	Domains	Resource-Development
T1041	Exfiltration Over C2 Channel	Exfiltration
T1590	Gather Victim Network Information	Reconnaissance
T1588.005	Exploits	Resource-Development
T1566	Phishing	Initial-Access
T1071.003	Mail Protocols	Command-And-Control
T1005	Data from Local System	Collection
T1113	Screen Capture	Collection
T1078.004	Cloud Accounts	Defense-Evasion

Sources

Source	URL	Tier
Security News	https://www.bleepingcomputer.com/news/security/fbi-warns-of-handala...	T3
Stryker attack raises concerns about role of device management tool	https://www.cybersecuritydive.com/news/stryker-attack-device-manage...	T3
Microsoft Intune: Lock it down, warn feds after Stryker - The Register	https://www.theregister.com/2026/03/19/microsoft_intune_lockdown_st...	T3
CISA urges US orgs to secure Microsoft Intune systems after Stryker ...	https://www.bleepingcomputer.com/news/security/cisa-warns-businesse...	T3
Lessons from the Stryker Incident - Sygnia	https://www.sygnia.co/threat-reports-and-advisories/identity-contro...	T3

DISCLAIMER

This intelligence report is produced by Tech Jacks Solutions Security Command Center (SCC) for informational purposes only. It does not constitute professional security advice, legal counsel, or an incident response engagement. The information herein is derived from publicly available sources and AI-assisted analysis; while every effort is made to ensure accuracy, Tech Jacks Solutions makes no warranties regarding completeness or timeliness. Organizations should conduct their own validation and consult qualified security professionals before taking action based on this report. Tech Jacks Solutions is not liable for any damages resulting from the use of this information.

Generated 2026-03-29 18:34 UTC by TJS Security Command Center