Stryker Corporation Cyberattack: Handala Wiper Incident

March 11th, 2026

Date	March 11, 2026
Victim	Stryker Corporation - Fortune 500 MedTech, HQ Kalamazoo, MI
Claimed Actor	Handala - Iran-linked hacktivist group, assessed as front for Void Manticore (Iranian state-sponsored)
Attack Type	Destructive Wiper Attack — Microsoft environment (Entra/Azure AD + Intune)
Stated Motive	Retaliation for U.S. missile strikes; broader US-Israel-Iran conflict
Reported Impacts	Factory resets of Intune-managed corporate laptops and workstations, factory resets of personal/BYOD phones where employees used Intune Work Profiles, loss of personal content on BYOD devices (photos, data, and eSIM details) for many employees.

Executive Summary

On March 11, 2026, medical device manufacturer Stryker Corporation confirmed a cyberattack causing a global disruption to its Microsoft environment. The Iran-linked hacktivist group Handala Hack claimed responsibility, stating the attack was carried out in retaliation for a U.S. missile strike on a school in Iran and the broader U.S.-Israel-Iran military conflict.

The attack is assessed as a destructive wiper operation, **not a ransomware event**. Stryker has stated there is no indication of ransomware or malware on their systems and believes the incident is contained. Employee reports and open-source intelligence indicate the following: corporate devices, servers, and phones were wiped clean, and employees were sent home from facilities in Ireland and the U.S. after losing access to work systems. Login screens on affected devices displayed the Handala logo.

Handala claims to have wiped more than 200,000 systems, servers, and mobile devices while also stealing 50 terabytes of company data. The group has a documented history of deploying wiper malware against Israeli targets since 2023 and has previously impersonated CrowdStrike in phishing campaigns. Reporting speculates that Stryker was likely targeted due to its 2019 acquisition of Israeli medical tech firm OrthoSpace and its contracts with the U.S. Department of Defense.

Who is Handala?

Handala Hack is an Iran-linked hacktivist group that has been highly active since the onset of the US-Israel-Iran conflict.

Handala is assessed as a potential front for Void Manticore, an Iranian government-sponsored threat actor known for phishing, data theft, custom wiper malware, and psychological warfare. Prior operations for Handala include attacks on Israeli military systems, government ministries, and civilian infrastructure across Israel, Jordan, and Saudi Arabia.

Some historical TTPs associated with this threat actor are:

- Proxy Execution via Regasm.exe
- Time Based Evasion via Ping – n
- Tasklist/ Findstr Execution to Search for Security Processes
- Suspicious Windows AutoIt3 Execution
- Wiper Attack

Impact

- Global manufacturing and business operations disrupted across U.S. and international sites, including Stryker's largest non-U.S. hub in Cork, Ireland (approximately 5,500 employees).
- All systems connected to the corporate network reported as down. Support staff, engineers, and administrative personnel sent home.
- Corporate email (Microsoft Outlook), phone systems, and internal platforms rendered inoperable. Phone systems returning automated messages citing a "building emergency."
- Employees who had linked personal devices to corporate systems (e.g., Outlook on personal phones) reported those personal devices were also wiped.
- The attack demonstrates that Iran-linked groups are willing and able to deploy destructive wipers against large multinational enterprises

Safeguards/Recommendations

The following recommendations are drawn from Health-ISAC's Threat Operations Center advisory related to the incident. They are general hardening and preparedness measures based on the claimed TTPs, not victim-specific guidance. MITRE ATT&CK and NIST CSF references are included as noted in the source.

1. **Identity & Admin Hardening**
    a. Inventory all Global Admin, Intune Admin, and Entra Admin accounts: Enforce strict least privilege and use specialized admin roles instead of 'Global Admin' wherever possible.
    b. Implement enhanced monitoring for privileged accounts in these systems. Ensure authentication activity, privilege use, and administrative access are comprehensively logged and monitored for suspicious, anomalous, or unauthorized behavior. Implement Conditional Access policies: Require compliant/hybrid-joined devices and strong MFA

for admin access. Limit admin sign-ins to known locations, devices, and dedicated admin workstations where possible.

c. Enforce strong MFA for all privileged accounts. Prefer phishing-resistant methods such as FIDO2 security keys or platform authenticators. Block legacy authentication and app passwords.
d. Implement Conditional Access policies for administrative access. Require strong MFA and compliant or hybrid-joined devices, and restrict admin access to known locations, trusted devices, and dedicated admin workstations wherever possible.
e. Enable and tune alerting for high-risk administrative changes and suspicious behavior, including creation, elevation, or modification of admin roles, suspicious sign-ins from atypical locations or devices, and administrative activity in critical platforms that could enable large-scale impact.

2. Intune & Device Management Controls

a. Verify that only tightly controlled roles can initiate destructive or high-impact administrative actions, including Device Wipe, Factory Reset, Autopilot Reset, Fresh Start, bulk policy pushes, or other commands that could affect large numbers of devices. Implement approval workflows or out-of-band verification for bulk or sensitive actions.
b. Separate BYOD devices from corporate-owned devices in Intune using distinct profiles, policies, and administrative controls. Limit the actions that can be performed against BYOD devices compared to managed corporate assets.
c. Confirm that detailed logs of all device management actions are retained and actively monitored, including who initiated wipe commands or policy changes, when the actions occurred, and which users or device groups were affected. Integrate Intune logs into the SIEM for correlation, anomaly detection, and incident investigation.
d. Confirm that detailed logs of all device actions are retained and monitored — including who initiated wipe commands, when, and against which device groups. Integrate Intune logs into your SIEM for correlation and anomaly detection.

3. Incident Response Preparedness for Cloud & MDM

a. Run tabletop exercises focused on compromise of privileged accounts in Entra ID or other high-impact control systems, malicious changes in Intune such as mass wipe or policy push activity, and loss of access to Microsoft 365, identity services, or core administrative platforms.
b. Document and test playbooks for rapid isolation and revocation of compromised admin credentials, containment of destructive administrative activity, use of emergency access or break-glass accounts, and escalation to Microsoft for tenant-level incident support when required.
c. Confirm that critical services, configurations, and administrative baselines are backed up, including device configuration baselines, key cloud and identity settings, and critical line-of-business applications, so recovery can proceed quickly after malicious or disruptive administrative actions.

References

- https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html

- https://thehill.com/policy/technology/5779368-stryker-iran-hack-schoo-strike/
- https://www.irishexaminer.com/news/munster/arid-41808308.html
- https://www.securityweek.com/medtech-giant-stryker-crippled-by-iran-linked-hacker-attack/
- https://therecord.media/stryker-cyberattack-iran-hackers
- https://www.reddit.com/r/cybersecurity/comments/1rqopq0/stryker_hit_by_handala_intune_managed_devices/