Handala Wiper Attack on Stryker: MOIS Hacktivists Destroy Medical Operations

Living-Off-the-Land MDM Abuse Disables Medical Technology Firm Across 79 Countries

Unofficial AI-assisted Research

Cloud Security Alliance AI Safety Initiative

2026-03-13

Key Takeaways

- On March 11, 2026, the Iranian MOIS-linked group Handala (attributed by multiple security researchers to MOIS and tracked as Void Manticore / Storm-0842) executed a global destructive cyberattack against Stryker Corporation, one of the world's largest medical technology companies, disabling operations across 79 countries.
- The attack did not use novel malware. Instead, threat actors abused Stryker's own Microsoft Intune MDM platform to issue legitimate remote wipe commands to more than 200,000 corporate and BYOD-enrolled devices simultaneously — a "living-off-the-land" technique that bypassed traditional endpoint security controls entirely.
- Handala claimed to have exfiltrated 50 terabytes of data prior to the wipe — a figure that has not been independently confirmed. Stryker's Lifenet EKG transmission system was disrupted, with Maryland reporting the system was non-functional statewide — a direct patient safety impact.
- Stryker filed an SEC regulatory disclosure acknowledging ongoing operational disruption with no known restoration timeline. CISA has launched a formal investigation.
- The attack establishes a new threat model for enterprise cloud environments: organizations that centralize endpoint management in cloud MDM platforms have created a single administrative control plane that, if compromised, can be weaponized for global-scale destruction in minutes.

Background

Stryker Corporation

Stryker Corporation is an American multinational medical technology company headquartered in Kalamazoo, Michigan. With FY2025 revenues of approximately $25.12 billion and a global workforce of roughly 56,000 employees, Stryker manufactures and distributes surgical equipment, orthopedic implants, neurotechnology systems, endoscopy devices, patient handling equipment, and emergency medical technology across more than 75 countries [1]. According to Stryker's corporate materials, the company's products reach an estimated 150 million patients annually, making it a critical node in the global healthcare supply chain [1]. Stryker's Lifenet platform, a networked system used by emergency medical services to transmit patient electrocardiogram data to receiving hospitals prior to arrival, is embedded in emergency cardiovascular care workflows across the United States.

In 2019, Stryker acquired Israeli orthopedic company OrthoSpace [3]. That acquisition would later be cited by Handala as justification for targeting the company, framing Stryker as a "Zionist-rooted corporation" and therefore a legitimate target in the group's stated political campaign.

Handala: Hacktivist Facade, State Weapon

Handala first emerged as a publicly visible persona in December 2023, presenting itself as a pro-Palestinian hacktivist collective borrowing the name and imagery of a beloved Palestinian political cartoon character created by Naji al-Ali. The group's public messaging – Telegram channels, defacement imagery, politically charged communiqués – is carefully constructed to suggest organic, decentralized activist origins. Security researchers have concluded this presentation is deliberately deceptive.

Check Point Research formally attributed Handala to Void Manticore in May 2024, in a report titled "Bad Karma, No Justice: Void Manticore Destructive Activities in Israel," establishing that the hacktivist persona is an operational cover for a destructive cyber unit inside Iran's Ministry of Intelligence and Security (MOIS) [4]. Microsoft tracks the same actor cluster as Storm-0842, and CrowdStrike uses the designation Banished Kitten [5][6]. Iranian researcher Nariman Gharib further identified the relevant internal MOIS structure as the Counter-Terrorism Division, led by Yahya Hosseini Panjaki – a MOIS deputy minister sanctioned by the U.S. Treasury Department in September 2024 [7]. Palo Alto Networks Unit 42 has assessed that the hacktivist framing serves to allow Iran to deny responsibility for its cyber operations while enabling state-directed destruction against political targets [8].

Prior to the Stryker attack, Void Manticore / Handala had established a documented pattern of destructive operations [22]. The group deployed the CL Wiper against Albanian government systems in July 2022 via a SharePoint exploitation chain, prompting the Albanian government to sever diplomatic relations with Iran [9]. The FBI and CISA jointly confirmed Iranian state attribution for that attack. More recently, the group deployed BiBi-Linux and BiBi-Windows wipers against Israeli targets following the October 7, 2023 Hamas attacks – malware designed to corrupt files with random data, manipulate partition tables, and append mocking ".BiBi" extensions referencing Israeli Prime Minister Netanyahu. The Stryker operation represents a significant tactical evolution: rather than deploying purpose-built destructive malware, the group weaponized the target's own enterprise infrastructure.

Security Analysis

Attack Methodology: Living Off the Land at Cloud Scale

The March 11, 2026 attack on Stryker followed what investigators describe as a multi-stage compromise of Stryker's Microsoft cloud environment [10][11]. Initial access appears to have been achieved through the compromise of privileged administrative credentials for Stryker's Microsoft Entra ID (formerly Azure Active Directory) environment, most likely via credential phishing or prior credential theft. Once inside the Entra environment with sufficient administrative privilege, the attackers accessed Stryker's Microsoft Intune tenant — the company's cloud-based unified endpoint management (UEM) platform used by IT administrators to manage, configure, and control enrolled corporate and BYOD devices across the organization.

Intune includes a legitimate administrative capability to issue remote wipe commands to enrolled devices, a feature designed to allow IT to protect corporate data on lost or stolen endpoints. The attackers issued mass remote wipe commands through this console, effectively enrolling the full scope of Stryker's global endpoint estate — estimated at over 200,000 devices — into a simultaneous destructive action. Because the wipe commands originated from a legitimate, trusted Microsoft cloud management service, traditional endpoint detection and response (EDR) tools would typically have no attack signature to detect, and network-based security controls would encounter no malicious traffic to block. The attack bypassed the conventional malware detection stack entirely — no malicious binary was executed, no exploit was triggered — by having the victim's own infrastructure perform the destruction [12].

Employee accounts across the United States, Ireland, Australia, and Costa Rica all reported identical experiences: devices became unresponsive simultaneously on the morning of March 11, with login screens replaced by Handala branding imagery. Stryker's Microsoft Entra login portal was simultaneously defaced with Handala graphics. Employees in affected offices reported reverting to pen-and-paper workflows as networked systems went offline [13]. BYOD-enrolled personal devices — employee-owned phones and laptops registered under Stryker's bring-your-own-device policy — were wiped alongside corporate equipment, resulting in personal data loss for individual employees.

The Data Exfiltration Dimension

Handala's post-attack communications claimed the exfiltration of 50 terabytes of data prior to executing the wipe [14]. This sequencing — exfiltrate, then destroy — is consistent with the group's documented operational playbook from prior campaigns and suggests the attackers maintained persistent access to

Stryker's environment for an extended reconnaissance and data collection phase before triggering the destructive phase. The 50 TB figure has not been independently confirmed, and Stryker's initial public statements did not address the exfiltration claim. The nature of the potentially exfiltrated data — which could encompass engineering documentation for medical devices, clinical trial data, manufacturing specifications, customer and patient records, or employee personal information — has significant downstream consequences that extend beyond the immediate operational disruption.

Healthcare Safety Implications

The disruption of Stryker's Lifenet platform represents the most immediate patient safety dimension of the attack [12][15]. Lifenet enables paramedics and emergency medical technicians to transmit 12-lead electrocardiogram data from the field to receiving hospitals before patient arrival, allowing interventional cardiologists to activate catheterization lab protocols in advance of STEMI (ST-elevation myocardial infarction) emergencies — a workflow that meaningfully reduces time-to-treatment in cardiac events by enabling catheterization lab activation before patient arrival. Maryland emergency management officials reported the system was non-functional across most of the state following the attack [12]. The full scope of healthcare system disruption across affected countries has not been publicly catalogued as of this writing.

Stryker's statement that the company saw "no indication of ransomware or malware" is technically accurate in the traditional sense: no ransomware payload was deployed, and no novel malicious binary was executed on victim systems. This framing, however, does not fully capture the operational reality that the company's own enterprise tooling was successfully weaponized by adversaries who had achieved privileged administrative control of its cloud environment. CISA has launched a formal investigation [16], and Stryker filed a material event disclosure with the U.S. Securities and Exchange Commission acknowledging ongoing operational disruption with no established restoration timeline [17].

Geopolitical Context and Stated Motivation

Handala's public communications framed the Stryker attack as retaliation for a February 28, 2026 U.S. military strike described by Handala as targeting a girls' school in Minab — a city in Hormozgan Province in southern Iran, which the group's communications erroneously characterized as being in Tehran — stating the strike killed at least 175 people, predominantly children [18]. The group also cited ongoing cyber operations against what it termed "the Axis of Resistance." Stryker was selected as the target on the basis of its 2019 OrthoSpace acquisition, which the group cited as evidence of the company's "Zionist-rooted" character. NBC News characterized the Stryker attack as the first significant instance of Iran targeting an American company since the start of the ongoing conflict [19].

This targeting logic — selecting a healthcare technology company for destruction based on a years-old acquisition of an Israeli firm — suggests an Iranian operational posture willing to target commercial organizations on the basis of Israeli business connections, a pattern warranting threat modeling attention from similarly situated organizations. The approach mirrors the use of similar justifications by Iranian-linked actors in prior destructive operations against Albanian government infrastructure (justified on the basis of Albania hosting MEK dissidents) and against Israeli civilian infrastructure following the October 7 attacks. Organizations with Israeli subsidiaries, partnerships, acquisitions, or supply chain relationships should assess their exposure to this targeting logic as an emerging risk factor [20].

Technical Indicators and TTPs

The Stryker attack, combined with Void Manticore's documented operational history, presents the following consolidated threat picture for defenders [21]:

Tactic	Technique	Relevance to Stryker Attack
Initial Access	Credential phishing / credential theft targeting Entra admins	Assessed primary vector
Privilege Escalation	Abuse of Global Administrator or Intune Service Administrator roles	Required for mass wipe capability
Execution	Intune remote wipe command via Microsoft Graph API or admin console	Confirmed destructive mechanism
Impact	Mass data destruction via legitimate MDM functionality	200,000+ devices wiped
Exfiltration	Bulk data collection prior to destruction phase	50 TB claimed; unconfirmed
Defacement	Microsoft Entra login portal modification	Confirmed
Lateral Movement	RDP abuse, tunneling tools (prior Void Manticore campaigns)	Prior TTPs; role in this attack unclear
Credential Harvesting	Mimikatz (documented in BiBi wiper investigations)	Prior TTPs

Recommendations

Immediate Actions

Organizations should immediately audit their Microsoft Entra and Intune administrative role assignments to identify accounts holding Global Administrator, Intune Service Administrator, or Device Administrator privileges. Any accounts with these roles that are not protected by hardware-backed phishing-resistant multi-factor authentication (MFA) — such as FIDO2 security keys or certificate-based authentication — represent an acute risk. Software-based TOTP authentication and SMS-based MFA are insufficient against credential phishing attacks targeting Entra administrative accounts, as these can be bypassed by adversary-in-the-middle phishing frameworks.

Conditional Access policies governing Entra administrative sessions should be reviewed and hardened. Administrative access to Intune should require compliant device status, named location restrictions where operationally feasible, and should not be accessible from unmanaged devices. Any historical sign-in and audit log activity in Entra and Intune should be reviewed for anomalous administrative actions, particularly any prior bulk device operations, policy modifications, or unusual sign-in patterns from unfamiliar IP addresses or locations.

Short-Term Mitigations

The Stryker attack demonstrates that the conventional perimeter between "malicious activity" and "legitimate administrative operation" has collapsed in cloud-managed environments. Organizations should implement a separation of duties model for destructive administrative capabilities: the Intune remote wipe function and similar high-impact operations should require approval from multiple named administrators, be restricted to dedicated privileged access workstations, and generate real-time alerts to a SIEM or security operations center when invoked. Privileged Identity Management (PIM) should be implemented in Entra ID to enforce just-in-time elevation for sensitive roles rather than persistent role assignment.

Logging coverage is equally critical. Microsoft Entra and Intune audit logs should be streamed continuously to an external, tenant-independent SIEM where they cannot be modified or deleted by a compromised tenant administrator. Specifically, the `DeviceRemoteAction` audit category in Intune — which records wipe and retire commands — should be monitored for volume anomalies, as the initiation of hundreds or thousands of simultaneous wipe operations would generate an unmistakable telemetry signal. Whether Stryker lacked such monitoring or was unable to act on telemetry before the wipe completed, the attack's outcome illustrates the necessity of monitoring this audit category for volume anomalies.

Healthcare organizations running Lifenet or equivalent prehospital telemedicine platforms should evaluate failover capabilities and protocols for extended platform unavailability. The cardiac care workflow dependency on Lifenet illustrated in this attack is representative of a broader pattern in which healthcare operations have acquired cloud service dependencies with inadequate offline contingency planning.

Strategic Considerations

The Stryker attack is most usefully understood not as a one-off event but as a proof of concept for a new class of large-scale destructive attack against enterprise cloud environments. The attack surface is not a specific vulnerability in Microsoft software — it is the architectural pattern of centralized, cloud-based endpoint management itself. Every organization that has consolidated endpoint control into a single cloud MDM tenant has, intentionally or not, created a single control plane whose compromise enables global-scale destruction with no novel malware required. This architectural risk deserves board-level attention and should inform cloud security architecture reviews with particular urgency in critical infrastructure sectors.

Organizations with Israeli business connections — subsidiaries, acquired companies, joint ventures, supply chain relationships — should reassess their threat model in light of the targeting logic evidenced by the Stryker attack. The years-old OrthoSpace acquisition was sufficient to qualify Stryker as a target in Handala's framing. This logic will likely be applied to other commercial organizations by Handala and potentially by other state-aligned Iranian threat actors operating under similar deniability constructs.

Finally, the potential 50 TB data exfiltration at Stryker carries implications that will outlast the operational disruption. Medical device engineering specifications, manufacturing processes, and clinical data represent high-value intelligence targets for a state that has strategically invested in healthcare and pharmaceutical intelligence collection. Organizations in the medical technology sector should assume that exfiltrated data from destructive attacks may be retained for intelligence purposes even when the primary stated motivation is political retaliation.

CSA Resource Alignment

This incident maps directly to multiple Cloud Security Alliance frameworks and guidance documents. The core failure mode — compromise of a privileged cloud identity leading to mass destructive action through legitimate administrative tooling — is addressed in CSA's **Zero Trust guidance**, which emphasizes that trust in cloud administrative actions must be continuously verified rather than assumed based on authentication alone. The principle of least privilege, with particular application to high-impact administrative capabilities such as MDM remote wipe, is a foundational Zero Trust control whose absence in Stryker's environment proved highly consequential.

CSA's **Cloud Controls Matrix (CCM)** control domains most directly applicable to this incident include Identity and Access Management (IAM), specifically controls governing privileged access governance (IAM-02), multi-factor authentication for administrative accounts (IAM-08), and audit logging for administrative actions (LOG-04 through LOG-08). The absence of separation of duties for destructive MDM operations maps to CCM control IAM-05. Organizations should conduct a CCM assessment scoped specifically to cloud identity and endpoint management administrative controls in the wake of this attack.

MAESTRO, CSA's threat modeling framework for agentic AI systems, is relevant as organizations increasingly deploy AI-driven endpoint management automation in their MDM environments. As AI agents are granted administrative capabilities equivalent to or exceeding those exploited in the Stryker attack, the same living-off-the-land risk surface expands: a compromised or manipulated AI agent with Intune administrative privilege could execute the same destructive action with greater speed and less detectable behavioral signature than a human operator. CSA's MAESTRO Layer 5 (Agent Control) guidance on constraining the blast radius of autonomous administrative actions should be incorporated into AI-augmented IT operations architectures.

The attack also has resonance with CSA's **AI Organizational Responsibilities** framework in the context of healthcare cloud security governance. Board-level accountability for cloud identity security posture — including the security architecture of centralized endpoint management platforms — is a governance obligation that the Stryker incident demonstrates carries patient safety dimensions, not merely operational or financial ones.

References

[1] Stryker Corporation, "FY2025 Annual Report," Stryker Investor Relations, 2026. https://www.stryker.com/us/en/about/investor-relations.html

[2] Wikipedia contributors, "Stryker Corporation," Wikipedia, accessed March 13, 2026. https://en.wikipedia.org/wiki/Stryker_Corporation

[3] Stryker Corporation, "Stryker completes acquisition of OrthoSpace," Press Release, 2019.

[4] Check Point Research, "Bad Karma, No Justice: Void Manticore Destructive Activities in Israel," Check Point Research Blog, May 2024. https://research.checkpoint.com/2024/bad-karma-no-justice-void-manticore-destructive-activities-in-israel/

[5] Microsoft Threat Intelligence, "Storm-0842" threat actor tracking designation, Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/ (specific profile page; date unavailable for public citation)

[6] CrowdStrike, "Banished Kitten" threat actor profile, CrowdStrike Adversary Intelligence. (Subscription required; see CrowdStrike Adversary Intelligence portal for full profile)

[7] N. Gharib, Iranian MOIS cyber unit attribution research, cited in Cyberint, "Handala Hack: What We Know About the Rising Threat Actor," Cyberint Blog. https://cyberint.com/blog/threat-intelligence/handala-hack-what-we-know-about-the-rising-threat-actor/

[8] Palo Alto Networks Unit 42, "Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran," Unit 42 Blog, March 2026. https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/

[9] CISA and FBI, "Iranian State Actors Conduct Cyber Operations Against the Government of Albania," Joint Advisory, September 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-264a

[10] BleepingComputer, "Medtech giant Stryker offline after Iran-linked wiper malware attack," BleepingComputer, March 11, 2026. https://www.bleepingcomputer.com/news/security/medtech-giant-stryker-offline-after-iran-linked-wiper-malware-attack/

[11] SecureWorld, "Iran-Linked Hacktivist Group Hits Stryker in Destructive Wiper Attack," SecureWorld News, March 2026. https://www.secureworld.io/industry-news/iran-linked-hacktivist-group-weaponizes-microsoft-intune-in-destructive-wiper-attack-on-stryker

[12] Krebs on Security, "Iran-Backed Hackers Claim Wiper Attack on Medtech Firm Stryker," KrebsOnSecurity, March 2026. https://krebsonsecurity.com/2026/03/iran-backed-hackers-claim-wiper-attack-on-medtech-firm-stryker/

[13] The Record (Recorded Future News), "Stryker cyberattack confirmed; Iran-linked Handala group claims responsibility," The Record, March 11, 2026. https://therecord.media/stryker-cyberattack-iran-hackers

[14] TechCrunch, "Pro-Iran hacktivist group says it is behind attack on medical tech giant Stryker," TechCrunch, March 11, 2026. https://techcrunch.com/2026/03/11/stryker-hack-pro-iran-hacktivist-group-handala-says-it-is-behind-attack/

[15] K. Zetter, "Iranian Hacktivists Strike Medical Device Maker Stryker in Severe Attack that Wiped Systems," Zetter Zero Day, March 2026. https://www.zetter-zeroday.com/iranian-hacktivists-strike-medical-device-maker-stryker-in-severe-attack-that-wiped-systems/

[16] Nextgov/FCW, "CISA launches investigation into Stryker cyberattack," Nextgov, March 2026. https://www.nextgov.com/cybersecurity/2026/03/cisa-launches-investigation-stryker-cyberattack/412079/

[17] Stryker Corporation, "A Message to Our Customers," Stryker News, March 2026. https://www.stryker.com/us/en/about/news/2026/a-message-to-our-customers-03-2026.html

[18] Al Jazeera English, "Iran-linked hackers hit medical giant Stryker in retaliatory cyberattack," Al Jazeera, March 11, 2026. https://www.aljazeera.com/news/2026/3/11/iran-linked-hackers-hit-medical-giant-stryker-in-retaliatory-cyberattack

[19] NBC News, "Iran appears to have conducted a significant cyberattack against a U.S. company," NBC News, March 11, 2026. https://www.nbcnews.com/world/iran/iran-appears-conducted-significant-cyberattack-us-company-first-war-st-rcna263084

[20] Flashpoint, "Destructive Activity Targeting Stryker Highlights Emerging Supply Chain Risks," Flashpoint Blog, March 2026. https://flashpoint.io/blog/destructive-activity-targeting-stryker-highlights-emerging-supply-chain-risks/

[21] Palo Alto Networks Unit 42, "Insights: Increased Risk of Wiper Attacks," Unit 42 Blog, March 2026. https://unit42.paloaltonetworks.com/handala-hack-wiper-attacks/

[22] HivePro, "Void Manticore: Iran's Evolving Cyber Warfare Model," HivePro Threat Advisory. https://hivepro.com/threat-advisory/void-manticore-irans-evolving-cyber-warfare-model/

