The Stryker “Wiper” Incident

March 2026

AutoTableTop™ 2.0 Facilitator Guide

Subject: Cyber-Sabotage, Administrative Tool Weaponization, Geopolitical Retaliation

Classification: CONFIDENTIAL — For Facilitator Use Only

Derezzed Inc. d/b/a ThreatGEN | info@threatgen.com | threatgen.com

Executive Summary

In March 2026, Stryker Corporation — a Fortune 500 medtech leader with $25.1B in revenue and operations across 79 countries — suffered one of the most consequential cyberattacks in corporate history. This was not ransomware. It was a state-aligned destructive wiper operation.

~200K
Devices Wiped

79
Countries Affected

50 TB
Data Claimed Exfiltrated

3 hrs
Attack Duration

Key Insight

The attack used no malware. No ransomware. No exploits. The attacker weaponized Microsoft Intune — Stryker's own endpoint management platform — to issue a mass factory-reset command. Every wipe was a legitimate, signed administrative action. EDR was architecturally blind.

Threat Actor: Handala

Void Manticore / Storm-1084 / MOIS-Directed

Attribute	Detail
State Sponsor	Iran — Ministry of Intelligence and Security (MOIS)
Doctrine	Combined “Hack-and-Leak” + “Wiper” operations. Goal: destruction, not profit.
Trigger	Feb 28, 2026 joint U.S.-Israeli “Operation Epic Fury” strikes in Tehran.
Targeting Rationale	U.S. military contracts + OrthoSpace Ltd. (Israeli subsidiary). Called Stryker “a Zionist-rooted corporation.”
Tool Overlap	Code linked to MuddyWater/Void Manticore. Front-end persona for state capabilities.
Historical Precedent	Saudi Aramco (Shamoon, 2012), Sands Casino (2014), Albanian gov (2022).
Claimed Impact	200K+ devices wiped, 50 TB exfiltrated. Published Rubrik & vSphere screenshots.

The Attack Chain: Intune Kill-Switch

Control Plane Compromise, Not Endpoint Compromise

02:00 EST

Initial Access

AiTM phishing captures authenticated session token. MFA bypassed — session hijack, not password theft.

03:15 EST

Privilege Escalation

Ghost Admin account created in Entra ID with Global Administrator privileges. Web shells planted for persistence.

04:00 EST

Detonation

Mass “Wipe” command issued via Intune to all enrolled devices. Native UEM function — signed, legitimate, trusted.

04:05 EST

Mass Impact

~200K devices factory-reset across 79 countries. Blue screens, login page defacement, total comms blackout.

Why Traditional Defenses Failed

EDR Blindness

The Wipe command is a signed, legitimate instruction from Microsoft's cloud. EDR treated it as an authorized admin action. Nothing to detect, block, or alert on.

MFA Bypass

Attackers stole the authenticated session token via AiTM reverse proxy. Once "in the session," the system assumed they were the trusted admin. MFA was completed by the real user.

No Malware Needed

Every destructive action was a legitimate administrative command. No files to scan, no signatures to match, no anomalous processes. Pure Living-off-the-Land.

"The most dangerous attack surface in a modern enterprise is not the endpoint — it is the identity and administrative control plane."

Target Profile: Stryker Corporation

Attribute	Detail
NYSE	SYK | Portage, Michigan
Revenue	$25.1 billion (2025)
Employees	~56,000 across 79 countries
Divisions	Orthopaedics | MedSurg & Neurotechnology | Spine
Key Products	Mako (robotic surgery), LIFEPAK, Vocera, SurgiCount, Airo TruCT, orthopedic implants
IT Environment	Microsoft-centric: Entra ID, Intune (UEM/MDM), M365, Azure. Hybrid with on-prem AD. BYOD enrollment.
Product Architecture	Connected medical devices on isolated, independent networks. Architecturally separated from corporate IT.
Targeting Exposure	U.S. military medical contracts + OrthoSpace Ltd. (Israeli subsidiary, acquired 2019).

Exercise Injects (1 of 3)

Inject #1: The Personal Privacy Crisis

T+30 min | Legal/HR

BYOD factory reset caused full device wipes on older OS versions. Thousands of employees lost personal photos and data. Employee posts go viral. Legal warns “Hold Harmless” clauses may not cover “Gross Negligence” if admin console was inadequately secured.

Pressure: Does your BYOD policy cover company liability when the MDM platform itself is weaponized? Should BYOD devices be in a separate Intune tenant?

Inject #2: The Clean Room Lockout

T+1 hr | Facilities/Ops

Badge readers and HVAC systems in implant manufacturing Clean Rooms authenticate via Entra ID. Systems fail-secure (locked). If HVAC offline >4 hours, $50M implant batch is contaminated and must be destroyed.

Pressure: Do your manufacturing environmental controls depend on the same identity provider as corporate IT? Network segmentation ≠ identity independence.

Exercise Injects (2 of 3)

Inject #3: The Ghost in the Machine

T+2 hrs | Trust/Security

Recovery team begins restoring from Rubrik backups. Handala posts on Telegram: “We saw you restoring the Finance DB. Thank you for doing the work for us. We’ve updated the admin password again.” Includes a screenshot with a timestamp from Stryker’s internal Rubrik console.

Pressure: You cannot restore into a compromised identity environment. Must build clean Entra ID tenant, revoke all sessions, rebuild identity infrastructure BEFORE restoring workloads.

Inject #4: The Surgical Supply Crisis

T+4 hrs | Supply Chain/PR

Personalized implants stuck in wiped shipping system. Surgeons threatening to cancel life-saving operations. Maryland EMS reports LIFENET ECG transmission offline statewide — paramedics using radio fallback.

Pressure: Do you restore the public website (press narrative) or the logistics SQL server (patient care)? When does EMS system downtime trigger FDA reporting?

Exercise Injects (3 of 3)

Inject #5: The Insider Doubt

T+6 hrs | HR/Security

Compromised admin account belongs to a senior IT employee who recently traveled to a country with known Iranian intelligence operations. Is this insider threat or phishing victim? HR wants immediate suspension; Legal warns of wrongful termination risk.

Pressure: How do you handle the human element during a nation-state investigation? Coordinate with FBI before employment action. Preserve forensic evidence. Don't prejudge.

Inject #6: The Media Firestorm

T+8 hrs | Comms/Executive

NBC breaks the story as first major Iranian cyberattack since war started. White House statement. Congressional briefing demands. Stock drops 4%. Major customer (8% of revenue) calls CEO asking about sourcing from a competitor.

Pressure: Who speaks publicly? How do you balance SEC disclosure requirements with operational security? How do you reassure major customers without promising recovery timelines?

Facilitator Pressure-Cooker Questions

Identity & Admin Controls

1. Do we have Wipe Protection thresholds in our UEM?
2. How long do admin session tokens last?
3. If Entra ID is compromised, can we verify our own staff OOB?
4. Are we using FIDO2/passkeys or push MFA?
5. Is Multi Admin Approval configured?

Recovery & Restoration

1. Can we rebuild Entra ID from scratch? How long?
2. Are backups in a system that authenticates through the compromised tenant?
3. How do we re-image 80K devices?
4. Can manufacturing sustain a 2-week outage?

Detection & Response

1. What telemetry catches a mass wipe in progress?
2. Do we monitor for new Global Admin creation in real-time?
3. What's our OOB comms plan if email/Teams are down?
4. How fast can we revoke all admin session tokens?

Organizational & Geopolitical

1. Does our BYOD policy cover MDM weaponization?
2. When does device infra downtime trigger FDA reporting?
3. Do we have pre-established FBI/CISA/ISAC relationships?
4. Would Feb 28 strikes have triggered elevated posture?

Win / Loss Conditions

Win Conditions

- Identifies attack as wiper (not ransomware) early
- Prioritizes identity containment before restoration
- Activates out-of-band communications
- Addresses BYOD personal device impact
- Prioritizes patient systems over PR/website
- Engages FBI/CISA/H-ISAC early
- Verifies backup integrity before restoring
- Develops coordinated external comms within 4 hrs

Loss Conditions

- Treats incident as ransomware
- Restores without verifying identity provider is clean
- Ignores BYOD personal device wipe
- Prioritizes PR/website over patient systems
- Uses compromised email/Teams for IR coordination
- Fails to engage law enforcement within 8 hours
- Takes premature employment action against compromised admin

Key Takeaways

1 Identity Is the New Perimeter

A single compromised privileged identity destroyed a $25B company's operations across 79 countries.

2 UEM Platforms Are Kill-Switches

Intune, JAMF, Workspace ONE — any platform with remote wipe authority is a potential weapon.

3 Phishing-Resistant MFA Is Not Optional

Only FIDO2/passkeys prevent AiTM session hijacking. Push and SMS MFA are insufficient.

4 Multi Admin Approval Is Critical

One admin wiping 80K devices with no secondary approval is a catastrophic single point of failure.

5 Wiper ≠ Ransomware

No decryption key. No negotiation. Total loss. Rebuild from identity infrastructure up.

6 Out-of-Band Comms Must Be Pre-Planned

When corporate email/Teams are down, you need Signal groups, sat phones, personal email lists.

7 BYOD = Shared-Fate Risk

Personal devices in corporate MDM share destruction risk. Assess whether BYOD enrollment benefits outweigh shared-fate.

8 Geopolitical Intel Is Operational

Military strikes → retaliatory cyber ops. Organizations with geopolitical exposure must elevate posture.

Thank You

For questions, licensing, or to schedule a live demonstration of AutoTableTop™ 2.0, contact us:

info@threatgen.com

threatgen.com