INTELLIGENCE BRIEFING
Security Command Center
TLP:CLEAR
2026-03-29 18:43 UTC

Iranian-Linked Hacktivist Group Claims Data-Wiping Attack Against Stryker

THREAT CAMPAIGN | HIGH

SCC Item ID	SCC-CAM-2026-0030
Type	Threat Campaign
Severity	HIGH
Affected Products	Stryker Corporation (specific systems and versions not confirmed in available data)
Published	2026-03-11

Executive Summary

An Iranian-affiliated hacktivist group has claimed responsibility for a wiper malware attack against Stryker Corporation, a major medical device and surgical technology manufacturer. The claimed attack involves data destruction, which carries potential for operational disruption, data loss, and supply chain concerns affecting healthcare sector partners. Attribution is unverified and based solely on the group's own claim; confirmed impact, scope, and affected systems have not been independently corroborated as of this report. **Current sourcing is T3 only (source quality score 0.64). This assessment is preliminary pending primary- or secondary-tier verification from CISA, law enforcement, or vendor threat intelligence.** Severity is rated high based on potential impact scope, not confirmed damage. If independent verification contradicts the claim, rating should be downgraded.

Technical Analysis

The group claims deployment of wiper malware against Stryker infrastructure. Mapped MITRE ATT&CK techniques include: T1485 (Data Destruction), T1486 (Data Encrypted for Impact), T1071 (Application Layer Protocol, likely for C2 communications), and T1583 (Acquire Infrastructure, consistent with pre-operation staging). No specific malware family has been confirmed. No malware sample has been recovered or analyzed. No CVE, CWE, or CVSS scoring applies to this campaign item. Affected systems, versions, and network segments are unconfirmed. Iranian hacktivist groups with intelligence agency affiliations have historically used wiper variants including ZeroCleare and Dustman; these are provided for context only and should not be interpreted as technical indicators for this claimed incident. Source quality score is 0.64 across T3 sources only; no primary or secondary tier sourcing is available at this time.

Action Checklist

1. Step 1 (Immediate): If your organization has direct network connectivity, data exchange, or vendor relationships with Stryker, assess exposure and consider temporary heightened monitoring or segmentation of that traffic pending confirmation of scope.
2. Step 2 (Detection): Hunt for wiper-associated behavioral indicators in endpoint telemetry, specifically mass file deletion events, MBR/VBR modification attempts, VSS shadow copy deletion (vssadmin delete shadows), and sudden large-volume write operations to disk.
3. Step 3 (Assessment): Inventory systems with connections to Stryker portals, EDI feeds, or shared network segments. Validate backup integrity and confirm last known-good restore points are isolated from production networks.
4. Step 4 (Communication): Brief leadership and relevant stakeholders on the unconfirmed nature of this claim. Avoid escalating to incident status without corroborating evidence, but document the watch item and assign an owner for ongoing monitoring.
5. Step 5 (Long-term): Review your third-party and supply chain risk posture for healthcare sector vendors. Validate that wiper-resilience controls are in place, offline or immutable backups, network segmentation, and endpoint protection coverage for destructive malware behaviors.

IR / Forensic Enrichment

Triage Priority	URGENT
Escalation Criteria	Escalate to management and external IR firm immediately if any IOC from the claimed Stryker attack is detected in your network, or if any unexplained mass file deletion, VSS shadow copy deletion, or MBR/VBR modification is observed on critical systems.
Recovery Notes	After containment, prioritize restoring systems from offline/immutable backups that predate the incident window. Validate all restored systems are scanning clean for IOCs before reconnecting to production. Rebuild compromised systems from golden images rather than restoring from potentially infected backups. Conduct a full forensic review of affected systems to understand initial compromise vector (supply chain, third-party access, credential theft) and remediate that vector to prevent recurrence.
Forensic Artifacts	Windows Security Event Log (Event IDs 4688, 4689, 4663, 4657 for process creation, file access/deletion, registry modification) | Sysmon logs (EventID 1 for process creation, EventID 10 for process access, EventID 23 for file deletion, EventID 3 for network connections) | NTFS Master File Table (MFT) and $UsnJrnl (USN journal) for file modification timeline | VSS shadow copy catalog and vssadmin logs for deletion attempts | Linux auditd logs and syslog for file operations, process execution, and system calls | Firewall/proxy logs for outbound connections from Stryker-connected systems during attack window | Browser history and cache from systems accessing Stryker portals (to identify potential watering-hole or supply chain compromise vectors) | Memory dump (if system still running) for volatile evidence of wiper malware in process memory

Per-Action IR Details

Step 1 (Immediate): If your organization has direct network connectivity, data exchange, or vendor relationships with Stryker, assess exposure and consider temporary heightened monitoring or segmentation of that traffic pending confirmation of scope.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.1 (preparation phase: tools and processes)

Controls: NIST 800-53 CA-7 (continuous monitoring), NIST 800-53 SI-4 (information system monitoring), CIS 6.2 (ensure network infrastructure is monitored for unusual activities)

Compensating: Query your network logs for all Stryker IP ranges and domains using grep/awk on firewall logs: `grep -E 'stryker|vendor_ip_range' /var/log/firewall.log | sort | uniq -c`. Export the connection matrix (source IP, destination IP, port, protocol, bytes transferred) to CSV and store offline. If no SIEM, run this daily and diff against baseline using `diff baseline.csv current.csv > deviations.txt`.

Evidence: Capture baseline network flow data (NetFlow/sFlow exports or firewall logs) for the past 30 days BEFORE implementing segmentation; document all Stryker-related connections by IP, domain, port, and protocol; preserve DNS query logs for any Stryker domains queried from internal hosts.

Step 2 (Detection): Hunt for wiper-associated behavioral indicators in endpoint telemetry, specifically mass file deletion events, MBR/VBR modification attempts, VSS shadow copy deletion (vssadmin delete shadows), and sudden large-volume write operations to disk.

NIST Phase: Detection Analysis

Reference: NIST 800-61r3 §3.2.4 (analysis: identifying indicators of compromise)

Controls: NIST 800-53 SI-3 (malicious code protection), NIST 800-53 SI-4 (information system monitoring), CIS 8.1 (implement application control on all systems), CIS 10.1 (capture and maintain audit logs)

Compensating: On Windows: query Event Log for mass deletions using `wevtutil qe Security /q:"*[System[(EventID=4689 or EventID=4688)]] and *[EventData[Data[@Name='CommandLine'] and (contains(., 'del ') or contains(., 'rm ') or contains(., 'cipher /w'))]]" /f:text > deletion_events.txt`. Monitor vssadmin calls: `Get-WinEvent -FilterHashtable @{LogName='Security'; ID=4688} | Where {$_.Message -match 'vssadmin'} | Export-Csv vss_attempts.csv`. On Linux: grep for mass file operations in auditd logs: `ausearch -k file_deletion | grep -E '(unlink|unlinkat|rmdir)' > file_ops.log`. For MBR/VBR: check for disk write activity via syslog: `grep -i 'write' /var/log/syslog | grep -E '(dev/sda|dev/hda|sector)' > disk_writes.log`.

Evidence: Before hunting: preserve Windows Security Event Log (Event IDs 4688, 4689, 4663 for file access/deletion), Sysmon logs (EventID 1 for process creation with vssadmin/cipher/del, EventID 23 for file deletion), MFT change journal ($UsnJrnl), and raw memory dump from suspect systems; on Linux preserve auditd logs, syslog, and /var/log/auth.log; capture full-disk image of any system showing these behaviors for offline forensic analysis.

Step 3 (Assessment): Inventory systems with connections to Stryker portals, EDI feeds, or shared network segments. Validate backup integrity and confirm last known-good restore points are isolated from production networks.

NIST Phase: Containment

Reference: NIST 800-61r3 §3.3 (containment) and §3.4 (eradication and recovery)

Controls: NIST 800-53 CP-9 (information system backup), NIST 800-53 CP-10 (information system recovery and reconstitution), NIST 800-53 SI-12 (information handling and retention), CIS 11.2 (ensure all data is backed up regularly)

Compensating: Create asset inventory manually: `netstat -ano | grep -E 'stryker|EDI_port_list' > connected_systems.txt` (Windows) or `netstat -tunap | grep -E 'stryker|EDI_port' > connected_systems.txt` (Linux). Document each system's backup schedule by interviewing backup admins and cross-referencing backup logs. Test restore on isolated VM: copy one backup file to quarantined test machine, attempt restore without connecting to production, and log success/failure with timestamps. Hash all backup media: `md5sum /mnt/backup/* > backup_hashes.txt` and store hashes in separate offline location.

Evidence: Preserve current network connectivity logs (arp -a output, routing tables via `route -n` or `Get-NetRoute`); capture backup metadata including last backup timestamp, backup file sizes, and backup media serial numbers; document the network isolation state of backup storage (physical disconnection status or air-gap confirmation); extract backup catalogs showing file inventory and last-modified dates.

Step 4 (Communication): Brief leadership and relevant stakeholders on the unconfirmed nature of this claim. Avoid escalating to incident status without corroborating evidence, but document the watch item and assign

an owner for ongoing monitoring.

NIST Phase: Preparation

Reference: NIST 800-61r3 §2.2 (tools and resources: communications and facilities)

Controls: NIST 800-53 IR-1 (incident response policy), NIST 800-53 IR-2 (incident response training), CIS 17.1 (establish incident response procedures)

Compensating: Create a watch-item tracking document (spreadsheet or text file) with columns: [Date_Reported, Threat_Title, Source, Confidence_Level (unconfirmed/suspected/confirmed), Systems_At_Risk, Last_Checked, Owner, Action_Items]. Email stakeholders with a templated brief: 'Iranian-linked group claimed attack on Stryker (unconfirmed). No evidence found in our environment to date. We are monitoring [specific indicators] for 7 days. Owner: [name]. Escalation threshold: detection of any IOC or corroborating industry intelligence.' Store this in a shared location with version history.

Evidence: Document the source of the threat claim (which vendor advisory, news outlet, or ISAC reported it), capture the original advisory text with URL and access date, record the date this communication was sent and to whom, and log all follow-up actions and monitoring results.

Step 5 (Long-term): Review your third-party and supply chain risk posture for healthcare sector vendors. Validate that wiper-resilience controls are in place, offline or immutable backups, network segmentation, and endpoint protection coverage for destructive malware behaviors.

NIST Phase: Post Incident

Reference: NIST 800-61r3 §3.5 (post-incident activities) and NIST 800-53 SR (supply chain risk management)

Controls: NIST 800-53 SR-3 (supply chain risk assessment), NIST 800-53 CP-9 (information system backup), NIST 800-53 SC-7 (boundary protection / network segmentation), CIS 2.2 (ensure proper network segmentation), CIS 11.2 (ensure all data is backed up regularly)

Compensating: Audit backup resiliency: for each critical system, document backup location, test restore RTO/RPO monthly, and confirm backups are disconnected from production (use network policies to block production-to-backup traffic, or physical disconnection). Validate network segmentation by running a VLAN/firewall audit: create a spreadsheet of critical systems and their allowed communication partners; validate with `tracert` (Windows) or `traceroute` (Linux) that traffic to non-approved peers is blocked. Test endpoint protection by running EICAR test malware signatures and confirming detection and quarantine. For compensating controls without EDR: enable file-access auditing on critical shares (Windows: audit object access on file system), enable process auditing on servers (Event ID 4688), and configure alerts for vssadmin/cipher/del commands via OSSEC or similar log monitoring.

Evidence: Collect backup audit logs for the past 12 months (successful/failed backup runs with timestamps and file counts), network segmentation documentation (firewall rules, VLAN assignments, ACLs), endpoint protection logs showing definition update frequency and detection history, and records of backup restore tests (date, system, RTO/RPO measured).

Detection Guidance

No confirmed IOCs are available for this campaign. Detection should focus on behavioral indicators consistent with MITRE T1485 and T1486. Key signals to investigate: (1) Processes invoking 'vssadmin delete shadows' or 'wbadmin delete catalog', common pre-wipe shadow copy removal. (2) Unusual volume of file overwrites or zero-byte writes across multiple directories in a short time window. (3) Drivers or processes attempting direct disk writes at the MBR or partition level (monitor for raw disk access outside of approved backup tools). (4) Outbound C2 traffic patterns consistent with T1071, irregular beacon intervals, non-standard ports, or connections to newly registered or low-reputation infrastructure. (5) If your SIEM or EDR supports it, create detections for known wiper execution patterns from CISA and MITRE ATT&CK group pages for Iranian-linked threat actors (APT33, APT34, OilRig as reference clusters). Note: these are precautionary behavioral hunts, not confirmed campaign-specific indicators.

Indicators of Compromise

Type	Value	Context	Confidence
DOMAIN	NOT AVAILABLE	No confirmed IOCs have been published or verified for this campaign as of this report. Do not use placeholder or speculative indicators.	LOW
URL	No confirmed IOCs available	No technical IOCs (IPs, domains, hashes, URLs) have been confirmed in available open sources for the Handala-Stryker incident. Attribution is based on actor self-reporting. Detection should rely on behavioral and log-based indicators described in detection_guidance.	LOW
URL	No confirmed IOCs published	No malware, hashes, C2 infrastructure, or network indicators have been publicly attributed to this specific Handala campaign against Stryker. Detection relies on behavioral and identity telemetry, not traditional IOC matching.	LOW

Framework Mappings

MITRE-ATTACK

- **T1071** — Application Layer Protocol
- **T1485** — Data Destruction
- **T1486** — Data Encrypted for Impact
- **T1583** — Acquire Infrastructure

NIST-800-53R5

- **CA-7** — Continuous Monitoring
- **SC-7** — Boundary Protection
- **SI-4** — System Monitoring
- **CP-9** — System Backup
- **CP-10** — System Recovery and Reconstitution

MITRE ATT&CK Mapping

Technique ID	Technique Name	Tactic
T1071	Application Layer Protocol	Command-And-Control

Technique ID	Technique Name	Tactic
T1485	Data Destruction	Impact
T1486	Data Encrypted for Impact	Impact
T1583	Acquire Infrastructure	Resource-Development

Sources

Source	URL	Tier
Krebs on Security	https://krebsonsecurity.com/	T3
Brian Krebs - SecureWorld News	https://www.secureworld.io/industry-news/author/brian-krebs	T3
Krebs on Security - Internet Salmagundi	https://internet-salmagundi.com/2019/12/krebs-on-security/	T3
Brian Krebs, the Cybersecurity Blogger Hackers Love to Hate - Reddit	https://www.reddit.com/r/netsec/comments/1vgd8x/brian_krebs_the_cyb...	T3
Krebs on Security - InfoSec Industry	https://infosecindustry.com/category/news/krebs-on-security/	T3
Security News	https://www.bleepingcomputer.com/news/security/stryker-attack-wiped...	T3
The Stryker Cyberattack: What This Means for Your ...	https://technologymatch.com/blog/the-stryker-cyberattack-what-this-...	T3
Deep dive into the Stryker cyberattack and the blind spot ...	https://shieldworkz.com/blogs/deep-dive-into-the-stryker-cyberattac...	T3
Lessons From The Stryker Attack: Securing Intune ...	https://youattest.com/blog/lessons-from-the-stryker-attack-securing...	T3
My boss wants to leave intune because of Stryker	https://www.reddit.com/r/cybersecurity/comments/1rvk7x6/my_boss_wan...	T3
The Stryker attack wiped 200K endpoints by abusing Intune's own ...	https://www.reddit.com/r/cybersecurity/comments/1rtmv5u/the_stryker...	T3

Source	URL	Tier
What the Stryker Attack Reveals About Endpoint Trust - Hexnode	https://www.hexnode.com/blogs/stryker-cyberattack-uem-security/	T3

Generated 2026-03-29 18:43 UTC by TJS Security Command Center