Stryker Cyber-Attack: What we Know so Far About the Remote Wipe Attack

By David Ketler

Published: 2026-03-27 · Archived: 2026-04-29 02:01:52 UTC

Table of Contents


stryker cyber-attack vsphere control panel

Table of Contents

- Stryker Cyber-Attack: What we Know so Far About the Remote Wipe Attack
- What happened in the Stryker cyber-attack?
- Chronological post-attack activity
- What we know about Handala
- What this means for defenders
- Defender strategies
- How Specops helps


David Ketler

On March 11, 2026, the Iranian hacktivist group **Handala Hack Team** claimed responsibility for a cyber-attack against the American healthcare technology company Stryker. According to public reporting, the attackers claimed to have impacted more than 200,000 systems and exfiltrated approximately 50 terabytes of data. While these figures remain unverified, the operational disruption alone places this incident among the more significant enterprise cyber-attacks of the year so far.

What happened in the Stryker cyber-attack?

Media reporting indicates that the attackers obtained Global Administrator-level access within Stryker’s Microsoft environment, giving them control over core administrative services, including endpoint management.

Bleeping Computer, citing an anonymous source described as familiar with Stryker's internal response, reported that the attackers may have used Microsoft Intune to issue remote wipe commands between approximately 5:00 and 8:00 a.m. UTC on March 11. An estimated 80,000 devices enrolled in Stryker's unified endpoint management service were reportedly impacted.

Because these actions appear to have been carried out through a legitimate administrative system, the disruption spread quickly. Employees across multiple regions reported devices being wiped overnight. Enrolled personal devices were also reportedly affected, resulting in the loss of personal data. As the activity became apparent, employees were instructed to power down devices in an attempt to limit further impact.

Stryker stated on March 15, 2026 that it remained confident its products and services were safe to operate and that no connected products had been compromised:

"This was not a ransomware attack, and there is no evidence of malware deployed to our systems. The incident has been contained, and we are now in the restoration process, which is progressing steadily."

How did Handala access Stryker?

How the attackers first gained access has not been confirmed. One possible explanation is the use of compromised credentials, potentially sourced from infostealer activity or other exposed authentication pathways. Supporting that possibility, threat intelligence researchers at Outpost24, Specops' parent company, identified compromised credentials associated with the stryker.com domain within its telemetry.

Between October 2025 and March 2026, a total of 278 compromised credentials were observed, with 138 linked to activity in 2026. Of these, 83 were observed in the pre-incident window between February 15 and March 11, corresponding to 31 unique email accounts. This shows a concentration of credential exposure in the weeks leading up to the attack, although it does not establish a direct link to the intrusion.

The majority of this activity was tied to Microsoft authentication endpoints, including:

- microsoftonline.com: 248 instances, primarily login.microsoftonline.com
- office365.com: 29 instances
- microsoft.com: 1 instance

This does not confirm the initial access vector, but it does show that exposed credentials linked to the organization were in circulation prior to the incident. It is also worth noting that Microsoft enforced multi-factor authentication on administrative accounts in late 2025.

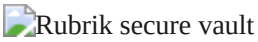
If an administrative account was involved, the attackers may have needed to steal a valid session or token or socially engineer an administrator into approving or surrendering MFA access. However, the exact sequence of events remains unconfirmed.

The incident reflects a broader pattern in which attackers abuse trusted administrative tools after gaining privileged access, instead of relying on ransomware or other traditional malware. In this case, the available reporting suggests that access to a privileged account, or successful privilege escalation, may have enabled remote wipe activity at scale.

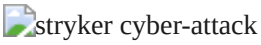
Chronological post-attack activity

March 16 2026

Handala published additional screenshots claiming significantly higher levels of impact, including the wiping of 12 petabytes of data and access to Rubrik Secure Vault backups and vSphere control panels.


Rubrik secure vault


vsphere control panel


stryker cyber-attack vsphere control panel

*Stryker's Rubrik Secure Vault and VSphere Control Panel that **Handala** supposedly accessed*

These claims remain unverified and should be treated with caution. As with many incidents involving destructive activity, attacker claims may be exaggerated to increase perceived impact.

It remains unclear whether Stryker was deliberately targeted or opportunistically compromised. Reporting by The Washington Post suggests the attack may have been framed by the group as part of a broader geopolitical narrative, although this has no bearing on the technical execution of the intrusion.

March 19 2026

Infrastructure associated with the group's public communications was seized by US law enforcement, including domains used to publish updates. While this may disrupt their ability to distribute messaging, it is unlikely to affect their operational capability.


fbi takedown notice

FBI takedown notice


Handala statement on website seizure

*Screen shot of **Handala's** response to its website take-down*

A second domain, Handala RedWanted, was also seized. In response, the group signaled its intent to continue operations and establish new infrastructure. Subsequent posts on its replacement site included retaliatory messaging linked to regional tensions, including threats of further action if Iranian power infrastructure was targeted and imagery claiming to identify Israeli critical infrastructure.

Handala's site has since returned, on the same registrar (with the same top-level domain) with a new domain name. On March 24, the group further escalated its rhetoric by publishing an unverified $50 million bounty threat against US President Donald Trump and Israeli Prime Minister Benjamin Netanyahu. These posts are more appropriately assessed as influence and intimidation activity than as reliable indicators of capability or intent.

March 26 2026

In an escalation of activity targeting US organizations, **Handala** claimed via Telegram to possess sensitive data linked to Lockheed Martin, a major US-based aerospace and defense company that designs, builds, and supports military and government systems.

In a related post, the group published personal data of 28 employees based in the Middle East, including names, addresses, and passport images. It alleged these individuals were involved in "critical" projects, including F-35 and F-22 maintenance, and shared supposed direct communications warning them to leave within 48 hours.

***Handala** Telegram post signaling alleged Lockheed Martin targeting*

Separately, a group identifying as **APT Iran** also claimed a breach of Lockheed Martin, alleging the exfiltration of 375 terabytes of data and demanding a $400 million ransom. The group claims to have copies of blueprints of F-35 aircraft, which is America's most advanced jet fighter, and other corporate information, according to Flashpoint.

A spokesperson for Lockheed Martin said the company is aware of the alleged claims.

"We are aware of the reports and have policies and procedures in place to mitigate cyber threats to our business," the spokesperson told Cybersecurity Dive via email. *"We remain confident in the integrity of our robust, multilayered information systems and data security."*

What we know about Handala

Handala is an online persona associated with a broader Iranian threat cluster linked to the Ministry of Intelligence and Security (MOIS). The group is also tracked by some vendors under names including **Void Manticore** and has been linked to a wider set of coordinated operations aligned with Iranian state interests.

The actor operates under other personas, including **Homeland Justice** and previously **Karma**, which have been used in campaigns targeting government, telecommunications, and critical infrastructure sectors, particularly in Albania and Israel.

The group's activity is characterized by the use of compromised credentials, manual access within victim environments, and the deployment of destructive actions such as wiping, deletion, and disk encryption. These operations are often accompanied by public claims and data leak activity.

Its reliance on widely available tooling and anonymized infrastructure, including commercial VPN services, makes its activity harder to attribute and limits the effectiveness of static indicators. Its operations tend to be short-lived, with a focus on speed and impact rather than persistence.

What this means for defenders

Attackers are shifting away from brute force and toward infostealer malware, which extracts high-value identity data directly from compromised endpoints, including credentials, session tokens, and access to SaaS and administrative portals.

These credentials are then sold or reused, allowing attackers to bypass perimeter defenses entirely. When a valid credential is used, especially one with administrative privileges, activity often appears legitimate and may not trigger controls such as MFA.

Defenders should review how conditional access and device compliance policies are enforced. In many environments, these controls are inconsistently applied or relaxed to reduce friction, allowing unmanaged or non-compliant devices to access corporate systems.

This incident also highlights a key limitation of tools like Microsoft Entra ID Password Protection. While effective at blocking weak passwords, they do not account for real-time credential exposure. As shown in Specops research, passwords that meet complexity requirements continue to appear in infostealer datasets.

Defender strategies

1. Enforce least privilege and privileged access governance

Administrative privileges should be minimized and segmented wherever possible. Implement just-in-time access, approval workflows, and session monitoring to reduce the risk of persistent high-level access being abused.

2. Validate device trust before granting access

Access decisions should not rely on identity alone. Devices requesting access to corporate resources should be continuously assessed for security posture, including patching status, configuration, and risk signals. This helps prevent compromised or unmanaged devices from being used as a launch point for further activity.

Specops Device Trust delivers that validation by authenticating both user and device at the point of access and throughout each session. Devices are checked continuously for issues like threats, outdated software and disabled security controls, giving teams full visibility into every device connecting to internal networks. Devices can be bound to specific identities, mitigating the risk of attackers using legitimate credentials on their own hardware.

3. Monitor and restrict use of administrative tooling

Enterprise management platforms such as endpoint management and remote administration tools should be treated as high-risk systems. Logging, alerting, and behavioral monitoring should be in place to detect unusual or large-scale actions, such as mass device wipes or configuration changes.

4. Improve visibility across identity and endpoint activity

Security teams should correlate identity events with endpoint and management plane activity to identify suspicious patterns early. Rapid detection of anomalous behavior, such as privilege escalation or unusual command execution, is key to limiting impact.

5. Plan, test, and rehearse for a worst-case scenario

Organizations should ensure that backups are secure, segmented, and regularly tested. Recovery plans should account for scenarios where administrative tools are abused, not just ransomware encryption events.

How Specops helps

The Stryker incident highlights a fundamental issue; access decisions are still too heavily reliant on identity alone.

Specops addresses this by combining breached password detection, secure resets, enforced MFA, and device-based access controls. This means that even if credentials are exposed, access is restricted to trusted users on trusted devices.

By validating both identity and device posture at login and throughout the session, these controls reduce the risk of administrative tooling being misused after initial access.

Download our white paper The Missing Piece in Zero Trust: Device Trust at Every Access Point to see how device trust strengthens access decisions across the full session lifecycle. Or contact us to learn how Specops can support your identity security strategy.

Last updated on **March 30, 2026**

Written by

David Ketler

David Ketler is a cybersecurity consultant based in Toronto, Canada with 10+ years of experience in software development and cybersecurity. He writes about password cracking, dark web activity, and password management.
