Update, March 13: Talos on the developing situation in the Middle East

By Cisco Talos

Published: 2026-03-03 · Archived: 2026-04-05 12:55:48 UTC

Monday, March 2, 2026 19:55

Update history

	Talos' assessment of the cyber attack on Stryker and the elevated threat landscape. Key findings and background on Handala, the Iranian-linked threat group.
	Updated guidance and recommendations, IOCs, and timelines.

Blog update: March 13, 2026

Executive summary

Cisco Talos assesses that the recent cyber attack on the medical equipment manufacturing firm, Stryker, likely represents an opportunistic compromise rather than a systematic shift toward targeting the health care sector specifically. Nevertheless, the broader threat landscape remains elevated due to ongoing military

operations in Iran, necessitating that all organizations increase vigilance and strengthen their defensive capabilities against destructive cyber activity.

Key findings

- Cisco Talos assesses that the publicly reported cyber attack on a U.S.-based medical equipment manufacturer, Stryker, likely does not indicate that the health care sector is at any higher or specific risk of targeting by Iran-linked threat actors. We make this assessment with high confidence based on our understanding of the motivation and capability of threat groups like Handala, which have historically compromised targets of opportunity. Talos has not observed any recent increase in systematic or elevated targeting of health care or health care-adjacent sectors over any other industry.
- Handala is an Iranian threat actor, which cybersecurity firms have linked to Iran's intelligence and security services, that conducts disruptive and destructive cyber operations under the guise of pro-Palestinian and pro-Iranian activism. The group combines low-level hacktivist activities with sophisticated techniques, including custom-made wiper malware and administrative tool hijacking, to execute high-impact attacks against global organizations.
- Despite our assessment that the health care sector is not at a higher risk specifically, the broader threat landscape remains elevated across all sectors amid ongoing military operations in Iran. Consequently, organizations are encouraged to reinforce their defensive postures and remain alert to destructive threats. Organizations should increase vigilance and evaluate their capabilities, encompassing planning, preparation, detection, and response for such an event.

Background

On March 11, 2026, the global medical technology firm Stryker was targeted in a cyber attack claimed by the Iran-linked threat group Handala, resulting in a severe disruption of its worldwide operations. The group asserts it deployed a destructive wiper attack to erase data from more than 200,000 systems — including servers, laptops, and employee mobile devices — and allegedly exfiltrated 50 terabytes of sensitive information in retaliation for recent military actions in Iran. This claim has not been officially verified. While Stryker has acknowledged a "global network disruption" to its Microsoft environment and is working with security partners to restore access, reports from its major hubs in the U.S. and Ireland indicate that the attack has effectively halted production and administrative functions, with many employees locked out of their devices.

We assess the attack was almost certainly executed by compromising high-level administrative accounts, based on our identification of hundreds of leaked Stryker credentials on the dark web. The threat actors likely gained access to Stryker's Microsoft Intune management console, within which they reportedly weaponized the platform's native remote wipe feature to simultaneously reset connected corporate devices. This living-off-the-land (LOTL) technique allowed the group to cause widespread destruction and data loss, possibly without the need for traditional wiper malware.

Handala: A state-linked threat group

The Handala group, also known as the Handala Hack Team, first emerged in December 2023, positioning itself as a pro-Palestinian hacktivist collective. Despite its hacktivist branding, leading cybersecurity firms assess the group

as a persona operated by Void Manticore (also known as Storm-0842 or Banished Kitten), a threat actor affiliated with the Iranian Ministry of Intelligence and Security (MOIS). This persona possibly allows the Iranian government to conduct destructive cyber operations while maintaining a degree of plausible deniability.

The group's operational history is defined by a rapid escalation from symbolic attacks to high-impact destructive campaigns. Initially, Handala focused almost exclusively on Israeli targets, claiming to have breached military weather servers, intercepted security feeds in Jerusalem, and compromised Telegram accounts allegedly associated with high-profile officials like former Prime Minister Naftali Bennett in "Operation Octopus." By 2025 and early 2026, the group expanded its scope to target Western organizations perceived as supporting Israel, culminating in the massive March 2026 attack on the medical technology giant Stryker.

Handala's tactics, techniques, and procedures (TTPs) blend state-sponsored capabilities with opportunistic hacktivist methods. They primarily gain initial access by accessing valid accounts, often through spear-phishing campaigns that exploit current events (such as the 2024 CrowdStrike outage) or by searching dark web sources for leaked credentials. Once inside, they often use hands-on-keyboard techniques to move laterally, reportedly demonstrating the ability to hijack administrative tools like Microsoft Intune to trigger remote factory resets on thousands of corporate devices simultaneously. Their arsenal includes custom-built wiper malware, such as Hatef (for Windows) and Hamsa (for Linux), often delivered via multi-stage loaders to evade detection. The group has also reportedly used commercial infostealer malware such as Rhadamanthys, according to industry reporting. To maximize psychological impact, they frequently pair these destructive acts with hack-and-leak operations, defacing victim websites and leaking sensitive data on their Telegram and dark web channels.

Recommendations for protection

Defend against destructive malware

Destructive malware, often leveraged by Iranian threat actors, can present a direct threat to an organization's daily operations, impacting the availability of critical assets and data. Disruptive cyber attacks against organizations in a target country may unintentionally spill over to organizations in other countries. Organizations should increase vigilance and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event. Refer to CISA's best practices for responding to destructive malware, outlined on pages 5 – 9 of their 2022 alert.

General best practices

Adhere to security fundamentals

An influx of threat actors of varying skill levels to this threat space may lead to unsophisticated methods being used to compromise victims, as we often see during times of conflict. Defenders should ensure security fundamentals are being adhered to, such as robust patching for known vulnerabilities, visibility into end-of-sale (EoS)/end-of-life (EoL) devices in your network with a plan to upgrade, and requiring multi-factor authentication (MFA) for remote access and on critical services. Patches for critical vulnerabilities that allow for remote code execution or denial-of-service on externally facing equipment should be prioritized. Organizations can also

implement a patch management program that enables a timely and thorough patching cycle. Talos' top security practices, including those to guide MFA deployment, can be found in our 2024 Year in Review report.

Blog update: March 10, 2026

Executive summary

On Feb. 28, 2026, the United States and Israel launched coordinated strikes against Iranian military and leadership targets, prompting Iranian missile and drone retaliation across the Middle East. Cisco Talos is closely monitoring the evolving cyber threat landscape associated with the conflict and collecting tactics, techniques, and procedures (TTPs); threat actor identifiers; and other intelligence to help inform defensive efforts and maintain situational awareness.

On March 8 2026, Iran's government selected Mojtaba Khamenei, the son of the late leader, as the new Supreme Leader; signaling a continuity of the regime's hardline policies. Talos assesses that, for the duration of this conflict, pro-Iranian cyber actors will likely continue targeting entities allied with the U.S. and Israel, primarily those located in the Middle East, with low-level attacks like denial-of-service (DoS), web defacements, and data leak campaigns. Furthermore, while the degree to which Iran's state-sponsored offensive capabilities have been degraded remains ambiguous, the regime maintains a historical capability and intent to execute disruptive ransomware and destructive wiper malware attacks against critical infrastructure (CI).

Outlook

Cyber operations are likely to play a supporting but strategically significant role in the ongoing conflict involving Iran, Israel, and the U.S. Given Iran's inability to match U.S. and Israeli conventional military capabilities, Tehran has historically relied on cyber operations conducted by both state-linked actors and aligned proxy groups as an asymmetric means of retaliation and influence. This pattern is again evident in the current conflict, with Iranian-aligned groups employing network-based intrusions to target adversary infrastructure and advance strategic objectives.

U.S. and Israeli operations reportedly compromised segments of Iran's information systems, yet the distributed nature of Iran's electronic warfare program across numerous agencies and proxies has likely provided a level of distributional resilience against these disruptions. While these targeted strikes likely slowed the overall operational tempo and forced a further shift in how capabilities are allocated across decentralized units, Iran likely retains some of its offensive online capacity and will likely continue leveraging digital intrusions as an asymmetric countermeasure.

Timeline

Though select hacktivist operations are highlighted below, hundreds of attacks have been claimed by numerous collectives since the beginning of the conflict. Talos cautions against accepting these claims at face value, emphasizing that defenders should independently verify them since older leaks and previously public information can be used to influence perceptions. The timeline below highlights higher-profile and more credible incidents.

- February
    - Between February and March 2026, the Iranian advanced persistent threat (APT) group Seedworm, who we track as MuddyWater (aka Temp Zagros, Static Kitten), targeted networks of multiple U.S. companies, including a bank, airport, and non-profit, as well as the Israeli operations of a U.S. software company. Seedworm deployed a previously unknown custom backdoor, named Dindoor, which leverages Deno, the secure runtime for JavaScript and TypeScript, to execute. They also deployed a Python backdoor named Fakeset.
    - Throughout February, Talos observed tools associated with Seedworm in the energy, education, and government sectors in Western countries. The tools include the aforementioned Dindoor, Fakeset, a backdoor named Darkcomp, and Stagecop (the loader for Darkcomp). A list of indicators of compromise (IOCs) associated with these tools can be found in the IOC section.
- February 28
    - Hacktivist group Sylhet Gang-SG claimed to have launched DDoS attacks targeting several entities, including: the Port of Los Angeles in the U.S.; the Qatari government's online portal, Ministry of Foreign Affairs, Ministry of Education, Ministry of the Interior, and Government Communications Office; Bahrain's airport and Information and eGovernment Authority; and the Abu Dhabi Civil Defense Authority in the United Arab Emirates (UAE).
    - Between February 28 and March 2, 2026, a coordinated surge of 149 hacktivist-attributed DDoS attacks targeted 110 organizations across 16 countries, occurring in the immediate aftermath of the U.S.–Israel military campaign against Iran.
    - Beginning on February 28, Iranian cyber actors significantly increased efforts to exploit internet-connected surveillance cameras in Israel and several Gulf states, leveraging known vulnerabilities to gain unauthorized access to live video feeds. Researchers assess the campaign likely sought to provide real-time situational awareness, reconnaissance, and battle damage assessment to support Iranian or proxy military operations.
- March 1
    - "Handala Hack," a hacktivist persona linked to Iran's Ministry of Intelligence and Security (MOIS), claimed to compromise Jordan Modern Oil & Fuel Services Co. Ltd. at the "mgc-gas[.]jo" website.
    - The Islamic Cyber Resistance in Iraq (aka 313 Team) claimed to have launched DDoS attacks targeting the official portal of the Jordanian government at "jordan[.]gov[.]jo" and the Kuwait Armed Forces website at "kuwaitarmy[.]gov[.]kw".
    - Hacktivist user "RipperSec" claimed to have launched a DDoS attack targeting the Israeli drone services provider at "propeller-drones[.]com".
    - "Investigation Anonymous" posted on their Telegram channel what they claim is an archive of leaked data of Israeli Defense Forces (IDF) personnel, including records from IDF training programs and personnel management systems.
    - Pro-Palestinian hacktivist group DieNet claimed to have launched DDoS attacks targeting several entities in the Middle East, including the Sharjah airport in the UAE, the Riyad and Al Rajhi banks in Saudia Arabia, the Oman government, and the Ras Al Khaimah airport in the UAE.
- March 2
    - The Iranian APTIran hacktivist group claimed on its Telegram channel to have compromised the state-owned food security agency Jordan Silos and Supply General Co. at the "josilos[.]com"

website. The breach allegedly occurred about a month earlier.
    - The Russia-aligned hacktivist group NoName057(16) pledged its solidarity with the Iranian regime in the ongoing armed conflict and claimed it started a DDoS attack campaign against Israel-based entities under the designator #OpIsrael. Targets include websites of political parties, local authorities, and telecommunications companies.
- March 8
    - Iran's government selected Mojtaba Khamenei, the son of the late leader, as the new Supreme Leader, signaling a continuity of the regime's hardline policies. He was considered the preferred candidate of the Islamic Revolutionary Guards Corps (IRGC), one of the most powerful political and military organizations in Iran, created to protect the regime's ideology and power.

Recommendations

Defend against destructive malware

Destructive malware, which Iranian threat actors often leverage, can present a direct threat to an organization's daily operations, impacting the availability of critical assets and data. Disruptive cyberattacks against organizations in a target country may unintentionally spill over to organizations in other countries. Organizations should increase vigilance and evaluate their capabilities encompassing planning, preparation, detection, and response for such an event. Refer to CISA's best practices for responding to destructive malware, outlined on pages 5 - 9 of their 2022 alert.

Limit publicly available data

The current conflict may prompt increased intelligence-gathering activity from cyber actors seeking to identify and exploit valuable targets. Espionage-focused actors often perform reconnaissance on targets' resources with the intent of gaining further information about their networks. Organizations should therefore consider minimizing the amount and sensitivity of data that is available to external parties. This can include scrubbing user email addresses and contact lists from public websites, which can be used for social engineering; sharing only necessary data with third parties; and monitoring and limiting third-party access to the network. Active scanning efforts can also be identified by monitoring network traffic for sources associated with botnets and adversaries, based on threat intelligence.

Enhance DDoS and website defacement protections

A more active hacktivist landscape inherently increases the threat of DDoS and website defacement attacks. To improve defenses against DDoS attacks, organizations should ensure they have a business continuity plan in place, assess their external attack surfaces, and confirm that critical systems have healthy, usable backups. For website defacement/redirect protection, ensure that websites are protected against the most commonly exploited security vulnerabilities, all forms or user inputs do not allow the injection of code into internal systems, secure application databases, and limit file uploads and the use of add-ons and plugins.

Adhere to security fundamentals

An influx of threat actors of varying skill levels to this threat space may lead to unsophisticated methods being used to compromise victims, as we often see during times of conflict. Defenders should ensure security fundamentals are being adhered to, such as robust patching for known vulnerabilities and requiring multi-factor authentication (MFA) for remote access and on critical services. Patches for critical vulnerabilities that allow for remote code execution or DoS on externally facing equipment should be prioritized. Organizations can also implement a patch management program that enables a timely and thorough patching cycle. Talos' top security practices, including those to guide MFA deployment, can be found in our 2024 Year in Review report.

Guidance on securing critical infrastructure

Network security teams should proactively monitor their traffic for APT-associated IP addresses. It is highly recommended to implement the hardening guidelines found in CISA's ST10-001 documentation and the Cybersecurity Resources Road Map, as these provide a foundational framework for securing network infrastructure against unauthorized access. Any traffic originating from malicious sources — particularly attempts to access remote work services like VPNs, webmail, or administrative interfaces for network hardware — should be treated as a confirmed threat. Furthermore, be aware of the risk posed by the technique identified as MITRE ATT&CK T0835. This involves the manipulation of Programmable Logic Controllers (PLCs), where an adversary alters the device's input/output data. This can cause the controller to ignore safety protocols or perform unintended physical actions, effectively breaking the link between digital control and physical reality. IRGC-affiliated threat actors have in the past exploited in multiple sectors in the U.S.

IOCs

The IOCs are also available on our GitHub repository here.

Seedworm domains/URLs:

- hxxps://iuumfgrrnuhb[.]zhivachkapro[.]com/pobor
- hxxp://terymar[.]com/install/Spf.ps1
- Elvenforest[.]s3.us-east-005.backblazeb2[.]com
- Uppdatefile[.]com
- Gitempire[.]s3.us-east-005.backblazeb2[.]com
- Moonzonet[.]com
- Serialmenot[.]com

Seedworm Loader Script:

- 29b777e7c5470d557e34f3b7b76d2ee291c2dfe7fbaee72821b53eb50a4062c8

Seedworm SHA256 associated with Dindoor:

- 0f9cf1cf8d641562053ce533aaa413754db88e60404cab6bbaa11f2b2491d542
- 1d984d4b2b508b56a77c9a567fb7a50c858e672d56e8cf7677a1fca5c98c95d1
- 2a00705cfd3c15cf8913e9eb4e23968efd06f1feceaef9987d26c5518887d043
- 2a09bbb3d1ddb729ea7591f197b5955453aa3769c6fb98a5ef60c6e4b7df23a5

- 42a5db2a020155b2adb77c00cbe6c6ad27c2285d8c6114679d9d34137e870b3f
- 7467f326677a4a2c8576e71a832e297e794ea00e9b67c4fcbe78b5aec697cec4
- 7c30c16e7a311dc0cdb1cdfd9ea6e502f44c027328dbe7d960b9bcd85ccf5eef
- b0af82de672d81f3c2f153977923b3884a8a9e7045b182c2379b19a1996931a0
- bd8203ab88983bc081545ff325f39e9c5cd5eb6a99d04ae2a6cf862535c9829a
- c7cf1575336e78946f4fe4b0e7416b6ebe6813a1a040c54fb6ad82e72673478e

Seedworm SHA256 associated with Fakeset:

- 077ab28d66abdafad9f5411e18d26e87fe43da1410ee8fe846bd721ab0cb52de
- 15061036c702ad92b56b35e42cf5dc334597e7311e98d2fdd3815a69ac3b1d84
- 2b7d8a519f44d3105e9fde2770c75efb933994c658855dca7d48c8b4897f81e6
- 4aef998e3b3f6ca21c78ed71732c9d2bdcc8a4e0284f51d7462c79d446fbc7be
- 64263640a6fdeb2388bca2e9094a17065308cf8dcb0032454c0a71d9b78327eb
- 64cf334716f15da1db7981fad6c81a640d94aa1d65391ef879f4b7b6edf6e7f1
- 94f05495eb1b2ebe592481e01d3900615040aa02bd1807b705a50e45d7c53444
- a4bd1371fe644d7e6898045cc8e7b5e1562bdfd0e4871d46034e29a22dec6377
- a5d4d6be3bfe0cba23fe6b44984b5fc9c7c7e10030be96120bb30da0f2545d4c
- ddceade244c636435f2444cd4c4d3dc161981f3af1f622c03442747ecef50888
- 74db1f653da6de134bdc526412a517a30b6856de9c3e5d0c742cb5fe9959ad0d

Seedworm SHA256 associated with Darkcomp:

- 1319d474d19eb386841732c728acf0c5fe64aa135101c6ceee1bd0369ecf97b6
- 3df9dcc45d2a3b1f639e40d47eceeafb229f6d9e7f0adcd8f1731af1563ffb90

Seedworm SHA256 associated with Stagecomp:

- 24857fe82f454719cd18bcbe19b0cfa5387bee1022008b7f5f3a8be9f05e4d14
- a92d28f1d32e3a9ab7c3691f8bfca8f7586bb0666adbba47eab3e1a8faf7ecc0

Original Blog - March 2, 2026

Cisco Talos continues to monitor the ongoing conflict in the Middle East. As always, we will be watching closely for any cyber-related incidents that are tied to the conflict. At this time we have not seen any significant cyber impacts, with some small incidents such as web defacements and small-scale distributed-denial-of-service (DDoS) attacks occurring. As with any highly fluid or dynamic situation, we are focused on providing our customers with highly accurate and timely intelligence and information.

Iranian groups involved in this conflict have historically operated primarily in the espionage, destructive attack, and hack-and-leak landscapes. We expect these, along with the mentioned activity, to be the most likely avenues in the near term.

Please see the following Talos research into regional actors in this area:

- Muddy Water, multiple campaigns
- Shrouded Snooper

Outlook on cyber activity

The data has thus far supported the belief that this will be a regional war with a large focus on kinetic activity, but that can change, we'll continue to monitor and will update accordingly. Currently there does not appear to be any significant increase in cyber activity associated with state-sponsored or state-affiliated groups.

Any possible impacts will likely be from sympathetic groups like hacktivists, some of whom have already launched website defacement and DDoS campaigns in support of Iran. Additionally, cyber criminals are likely to take advantage of the war to try and increase their scope of infections through the use of lures and other social engineering avenues. Users are reminded to be vigilant when clicking links and opening documents, as it is common for criminals to leverage these conflicts as cover for monetary gain.

Talos is well-versed in monitoring wartime environments with our ongoing work in Ukraine and across the globe. We will remain vigilant looking to identify any cyber related activity relevant to the region. If and/or when more relevant information becomes available, we will update this blog accordingly.

Guidance

Recommendations for organizations are currently focused on security hygiene, to include having multi-factor authentication (MFA) enabled, being diligent around any links or documents that are circulating, and ensuring you have proper monitoring in place to ensure you are prepared for any collateral impacts as they arise.

Since this activity appears to be regionally focused, making sure enterprises are aware of any impacts to partners and third-party suppliers in the region will be paramount. Additional inspection or controls may be warranted to insulate potential larger impacts to the wider organization.

Employee awareness: Beware of "hacktivist" lures

- Warn employees against clicking on unsolicited links related to the Middle East conflict, whether news or humanitarian. These are often infostealers or backdoors in disguise and meant to take advantage of emotions.
- Increase the frequency of phishing simulations that use current geopolitical lures to keep staff vigilant against social engineering.

Third-party risk assessment

- Map your dependencies. Identify any vendors, service providers, or developers located in or heavily connected to the Middle East conflict zone.
- Enforce strict MFA for all third-party access and conduct "zero-trust" audits on any administrative tools that have deep access to your environment.

Mitigate "nuisance" attacks and defacements

- Protect your public-facing brand. Use a Content Delivery Network (CDN) with robust DDoS mitigation and ensure all web content management systems (CMS) are fully patched.

As always, ensure all software has been updated to the latest versions to minimize the attack surface and ensure you have a robust patching process. Many updated software versions have improvements in security and visibility capabilities that can help in cyber defense.
