

U.S. Agencies Warn of Rising Iranian Cyber Attacks on Defense, OT Networks, and Critical Infrastructure

By The Hacker News

Published: 2025-06-30 · Archived: 2026-06-04 02:00:59 UTC



U.S. cybersecurity and intelligence agencies have issued a joint advisory warning of potential cyber attacks from Iranian state-sponsored or affiliated threat actors.

"Over the past several months, there has been increasing activity from hackers and Iranian government-affiliated actors, which is expected to escalate due to recent events," the agencies [said](#).

"These cyber actors often exploit targets of opportunity based on the use of unpatched or outdated software with known Common Vulnerabilities and Exposures or the use of default or common passwords on internet-connected accounts and devices."

There is currently no evidence of a coordinated campaign of malicious cyber activity in the U.S. that can be attributed to Iran, the Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), the Department of Defense Cyber Crime Center (DC3), and the National Security Agency (NSA) noted.

Emphasizing the need for "increased vigilance," the agencies singled out Defense Industrial Base (DIB) companies, specifically those with ties to Israeli research and defense firms, as being at an elevated risk. U.S. and Israeli entities may also be exposed to distributed denial-of-service (DDoS) attacks and ransomware campaigns, they added.

Attackers often start with reconnaissance tools like Shodan to find vulnerable internet-facing devices, especially in industrial control system (ICS) environments. Once inside, they can exploit weak segmentation or misconfigured firewalls to move laterally across networks. Iranian groups have previously used remote access tools (RATs), keyloggers, and even legitimate admin utilities like PsExec or Mimikatz to escalate access—all while evading basic endpoint defenses.



Based on prior campaigns, attacks mounted by Iranian threat actors leverage techniques like automated password guessing, password hash cracking, and default manufacturer passwords to gain access to internet-exposed devices. They have also been found to employ system engineering and diagnostic tools to breach operational technology (OT) networks.

The development comes days after the Department of Homeland Security (DHS) [released](#) a bulletin, urging U.S. organizations to be on the lookout for possible "low-level cyber attacks" by pro-Iranian hackers amid the ongoing geopolitical tensions between Iran and Israel.

Last week, Check Point [revealed](#) that the Iranian nation-state hacking group tracked as APT35 targeted journalists, high-profile cyber security experts, and computer science professors in Israel as part of a spear-phishing campaign designed to capture their Google account credentials using bogus Gmail login pages or Google Meet invitations.

As mitigations, organizations are advised to follow the below steps -

- Identify and disconnect OT and ICS assets from the public internet
- Ensure devices and accounts are protected with strong, unique passwords, replace weak or default passwords, and enforce multi-factor authentication (MFA)
- Implement phishing-resistant MFA for accessing OT networks from any other network
- Ensure systems are running the latest software patches to protect against known security vulnerabilities
- Monitor user access logs for remote access to the OT network
- Establish OT processes that prevent unauthorized changes, loss of view, or loss of control
- Adopt full system and data backups to facilitate recovery

For organizations wondering where to start, a practical approach is to first review your external attack surface—what systems are exposed, which ports are open, and whether any outdated services are still running. Tools like [CISA's Cyber Hygiene program](#) or open-source scanners such as Nmap can help identify risks before attackers do. Aligning your defenses with the MITRE ATT&CK framework also makes it easier to prioritize protections based on real-world tactics used by threat actors.



"Despite a declared ceasefire and ongoing negotiations towards a permanent solution, Iranian-affiliated cyber actors and hacktivist groups may still conduct malicious cyber activity," the agencies said.

Update

In a new report, Censys said it uncovered 43,167 internet-exposed devices from Tridium Niagara, 2,639 from Red Lion, 1,697 from Unitronics, and 123 from Orpak SiteOmat as of June 2025. A majority of the increased exposures associated with Tridium Niagara appear to be in Germany, Sweden, and Japan.

It also noted that default passwords continue to provide an easy pathway for threat actors to access critical systems, urging manufacturers to avoid shipping devices or software with default credentials, and instead require strong, unique passwords as well as offer ways to prevent exposing their systems directly to the internet.

"Apart from Unitronics, which is most commonly observed in Australia, the highest numbers of these devices are observed in the U.S.," the company [said](#). "Though Tridium Niagara boasts the highest exposure numbers, it's building automation software. Depending on a threat actor's objective, these systems, though plentiful, may not be the most valuable targets."

SOCRadar [said](#) the Iran-Israel conflict of 2025 has led to a spike in cyber activity, with more than 600 cyber attack claims reported across more than 100 Telegram channels between June 12 and 27, 2025. Israel emerged as the most targeted country with 441 attack claims, followed by the U.S. (69), India (34), and Middle Eastern nations like Jordan (33) and Saudi Arabia (13).

The top hacktivist groups during the time period included Mr Hamza, Keymous, Mysterious Team, Team Fearless, GARUDA_ERROR_SYSTEM, Dark Storm Team, Arabian Ghosts, Cyber Fattah, CYBER U.N.I.T.Y, and NoName057(16). Governments, defense, telecom, financial services, and technology sectors were among the most targeted industries.

"Since the war began, state-sponsored hackers, hacktivists from both countries, and cyber actors from non-participant nations ranging from South Asia to Russia to across the Middle East have become active," the threat intelligence firm [said](#). "Israel was the main target of DDoS attacks, with 357 claims, making up 74% of all DDoS activity."

Highlighting the surge in hacktivist activity amid the conflict, Outpost24 KrakenLabs researcher Lidia López Sanz said over 80 distinct hacktivist groups are "actively conducting or supporting" offensive cyber operations targeting Israel and its allies, adding suspected [faketivist entities](#) such as Cyber Av3ngers, Handala, and Predatory Sparrow are likely operating with state support or directly under state direction.

Among the hacktivist collectives that have expressed solidarity with Iran are DieNet, Mysterious Team Bangladesh, Team Insane Pakistan, Z-Alliance, Server Killers, Akatsuki Cyber Team, GhostSec, Keymous+, Inteid, Anonymous Kashmir, and Mr Hamza Cyber Force.

"The dramatic rise in hacktivist cyber operations following recent geopolitical escalations between Israel and Iran underscores the increasingly central role cyber conflict plays within modern warfare," Outpost24 [said](#).

"Ideologically-driven hacktivists, alongside possible nation-state faketivists, have clearly demonstrated their readiness to exploit geopolitical tensions to pursue diverse strategic objectives."

Found this article interesting? Follow us on [Google News](#), [Twitter](#) and [LinkedIn](#) to read more exclusive content we post.

Source: <https://thehackernews.com/2025/06/us-agencies-warn-of-rising-iranian.html>