SECURITY ADVISORY

MARCH 13, 2026

IRANIAN BACKED CYBER THREAT ACTIVITY TARGETING U.S. ORGANIZATIONS

SENTINELBLUE

OVERWATCH

BLUF (BOTTOM LINE UP FRONT)

Recent intelligence released by the Cybersecurity and Infrastructure Agency (CISA), the Federal Bureau of Investigation (FBI), and the National Security Agency (NSA) indicates that Iranian government-sponsored and affiliated cyber actors pose an elevated cyber threat to U.S. organizations amid the ongoing geopolitical conflicts in the Middle East.

Iranian cyber operations frequently involve social engineering, credential compromise, software exploitation, distributed denial-of-service (DDoS) attacks, ransomware deployment, and data exfiltration operations. These campaigns commonly rely on exploitation of known vulnerabilities in widely deployed enterprise technologies rather than sophisticated zero-day attacks.

Common attack vectors include compromised credentials obtained through phishing campaigns or password-spraying attacks, as well as exploitation of internet-facing enterprise services that have not yet been patched against publicly disclosed vulnerabilities.

The Sentinel Blue Overwatch team reviewed publicly available intelligence and recent reporting related to Iranian cyber operations to provide awareness of the techniques, vulnerabilities, and attack patterns currently associated with these campaigns.

As geopolitical tensions evolve, organizations should remain vigilant and maintain heightened awareness of suspicious activity across authentication systems, externally exposed services, and employee communications.

THREAT LANDSCAPE & IRANIAN TRADECRAFT

These prominent Iranian campaigns have expanded significantly over the past decade, now involving a “triple threat” of state-sponsored threat actors, proxy organizations, and ideologically motivated hacktivist groups. During periods of heightened geopolitical tension, these actors have increased attacks targeting organizations perceived to hold strategic, economic, or symbolic value–extending to government services, critical infrastructure, healthcare, communications, transportation, and defense-related manufacturing industries.

Iranian tradecraft has historically relied on opportunistic intrusion techniques targeting weak authentication, unpatched software, and exposed services to gain initial access. However, recent reporting from Reuters and Palo Alto's Unit 42 highlights a significant shift toward more destructive, high-impact operations. On March 11th, medical tech giant Stryker fell victim to a Iran-linked cyber-attack that led to the remote wiping of thousands of employee devices.[i]

Further analysis by Unit 42 notes that Iranian-aligned actors are also leveraging identity-driven access and artificial intelligence (AI) to accelerate the attack lifecycle. These campaigns often bypass traditional perimeters by exploiting over-scoped identities and software supply chain vulnerabilities. According to CISA, over a hundred common vulnerabilities and exposures (CVEs) have been associated with Iranian Advanced Persistent Threat (APT) groups, affecting common enterprise platforms such as Microsoft Exchange, VMware, and Fortinet. [ii]

As these actors integrate into broader cybercriminal ecosystems, the risk has escalated from simple lateral movement to severe operational disruption and public exposure of sensitive information.[iii]

DOCUMENTED CAMPAIGN ACTIVITY

Several recent incidents illustrate the types of operations commonly attributed to Iranian-aligned threat actors:

Healthcare Sector - Stryker

Iranian-linked threat actors claimed responsibility for a cyberattack targeting Stryker, a major U.S.-based medical device manufacturer. The attack reportedly disrupted portions of the company's information technology infrastructure and impacted systems used for order processing and manufacturing operations.

Although the exact intrusion methods were not publicly disclosed, Iranian cyber campaigns targeting enterprise organizations frequently begin with phishing attacks (MITRE ATT&CK T1566) or password-spraying attempts against externally accessible authentication services (T1110.003). These access methods allow attackers to obtain valid credentials (T1078) and gain access to corporate systems without immediately triggering traditional security alerts.

Municipal Infrastructure - U.S. Water Facilities

Iranian-affiliated hacktivist groups have also claimed responsibility for intrusions affecting small municipal water systems in the United States. Public reporting indicated that attackers gained access to internet-connected control systems using exposed credentials and unsecured remote access services.[iv]

Public reporting indicated that the device was accessible through an internet-connected management interface and was using default or exposed credentials. Iranian-aligned actors have historically exploited similar weaknesses using techniques such as exploitation of internet-facing systems (T1190) or credential-based access through exposed remote management services (T1110).

Financial Sector - Distributed Denial-of-Service Campaigns

Iranian cyber actors have historically conducted distributed denial-of-service (DDoS) campaigns targeting financial institutions and government organizations. These operations attempt to overwhelm publicly accessible services with large volumes of traffic, disrupting online banking platforms and public-facing services while creating reputational and operational impacts for targeted organizations.[v]

These operations relied on distributed denial-of-service activity (T1498) in which attackers directed massive volumes of network traffic toward targeted services. Although the primary objective of the campaign was service disruption rather than network compromise, the attacks demonstrated the ability of Iranian cyber actors to coordinate large-scale infrastructure capable of impacting critical financial services.

Defense Sector - Aerospace & Defense Espionage Campaigns

Iranian state-aligned cyber groups have conducted cyber espionage campaigns targeting aerospace and defense organizations. Public reporting indicates that attackers frequently impersonated employees or suppliers in phishing campaigns and targeted organizations involved in aircraft manufacturing, satellite technology, and defense logistics. These operations were primarily aimed at collecting sensitive technical information and research data rather than causing immediate operational disruption.[vi]

Public threat intelligence reporting indicates that these campaigns frequently rely on spear-phishing emails designed to harvest credentials (T1566) or deliver malicious attachments. After gaining access to employee accounts, attackers may leverage valid credentials (T1078) and attempt to move laterally across internal systems using remote services (T1021) to collect intellectual property or engineering data.

DEFENSIVE CONSIDERATIONS

Organizations can reduce exposure to opportunistic cyber campaigns by maintaining strong baseline cybersecurity practices.

RECOMMENDED DEFENSIVE MEASURES:

- **Enforcing** multi-factor authentication (MFA) for remote access services.
- **Monitoring** authentication activity for abnormal login behavior or impossible travel events.
- **Applying** vendor security updates to internet-facing systems as soon as patches become available.
- **Limiting** exposure of administrative services such as RDP or SSH to the public internet.
- **Conducting** employee awareness training to help identify phishing attempts and suspicious communications.

During periods of geopolitical tension, organizations should remain alert for social engineering attempts or suspicious login activity that may indicate opportunistic intrusion attempts.[vii]

---

[i] Iran-linked hackers claim responsibility for attack on US medical device maker Stryker. AJ Vicens, Christy Santhosh. March 11, 2026.
[ii] Iran Threat Overview and Advisories. CISA. June 30, 2025.
[iii] Threat Brief: March 2026 Escalation of Cyber Risk Related to Iran. Unit 42. March 2, 2026.
[iv] Iranian hacker group CyberAv3ngers allegedly breach Municipal Water Authority of Aliquippa. Anna Ribeiro. November 27, 2023.
[v] Iranians Charged with Hacking U.S. Financial Sector. Federal Bureau of Investigation. March 24, 2016
[vi] Insights into Iranian Cyber Espionage. Jacqueline O'Leary, Josiah Kimble, Kelli Vanderlee, Nalani Fraser. September 20, 2017.
[vii] Inside the Shadows: Understanding Active Iranian APT Groups. Huseyin Can Yuceel. July 3, 2025.