

CISA Urges Continued Vigilance Amid Conflict with Iran

Amid the ongoing conflict, Iranian government-sponsored and -linked cyber threat actors continue to pose a heightened risk to U.S. critical infrastructure. These actors have demonstrated the capability and intent to target U.S. critical infrastructure sectors and companies, both domestically and abroad. To strengthen national readiness and response, the Cybersecurity and Infrastructure Security Agency (CISA) is conducting enhanced coordination with federal partners, including the Department of War and the Federal Bureau of Investigation, to identify threats and reduce risk.

Sustained vigilance remains essential to identifying and responding to potential malicious activity. Historically, Iranian government-sponsored and -linked cyber threat actors have targeted the following sectors, with the intent to disrupt services, exfiltrate data, and inflict reputational damage:

- Government Services and Facilities
- Water and Wastewater Systems
- Defense Industrial Base
- Energy
- Transportation Systems (including Aviation)
- Financial Services
- Communications
- Healthcare and Public Health

Iranian government-sponsored and -linked cyber threat actors commonly use the following tactics and techniques to achieve their goals:

- **Credential Abuse and Access Exploitation:** Use of brute force, password spraying, and credential stuffing against internet-accessible services to compromise accounts and gain access to internal networks. These tactics are exacerbated by weak or default passwords, unprotected remote access, and lack of multi-factor authentication (MFA).
- **Industrial Control Systems (ICS)/Operational Technology (OT) Targeting:** Scanning and exploitation of exposed ICS devices such as programmable logic controllers, and the misuse of legitimate tools to interact with OT remain consistent with tactics observed in prior intrusions and often target unprotected ICS and OT environments.
- **Ransomware and Data Leak Operations:** Possible collaboration with criminal organizations to deploy ransomware or exfiltrate sensitive information for leverage or tactical advantage. Actors may conduct follow-on information-leak campaigns, with some exaggerating the scale, meaning, or importance of stolen data.
- **Distributed Denial-of-Service Campaigns:** Targeted distributed denial-of-service campaigns against public-facing services and websites intended to degrade availability and create cascading impacts, particularly when traffic filtering and rate-limiting protections are absent or insufficient.

Given the threat environment, CISA urges critical infrastructure owners and operators, law enforcement, first responders, and state, local, tribal, and territorial governments to implement the following recommended risk-reduction measures to harden critical infrastructure:

- Eliminate unnecessary remote access by disabling Remote Desktop Protocol and administrative remote access unless explicitly required and enforcing MFA for privileged accounts.
- Reduce non-essential services and limit attack surface by disabling unused ports, protocols, and services; removing default or unused accounts; and segmenting critical systems such as ICS/OT from general business networks.
- Improve detection and monitoring capabilities for faster identification of malicious activity. Enable logging and real-time monitoring, maintain up-to-date anti-malware tools, and deploy intrusion detection or prevention systems where feasible.
- Implement strong patch and vulnerability management practices. Prioritize remediation of [known exploited vulnerabilities](#) identified by CISA and leverage [available alerting](#) and [cyber hygiene services](#).
- Maintain offline backups, test restoration procedures, and ensure manual control contingencies for ICS/OT environments to sustain operations during and after an incident.
- Establish clear incident response roles and ensure unusual activity is escalated quickly.

To strengthen defenses against Iranian government-sponsored and -linked cyber threat actors, network defenders can review the following resources for mitigation guidance and additional information:

- [Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest](#)
- [Iran Threat Overview and Advisories](#)
- [Understanding and Responding to Distributed Denial-of-Service Attacks](#)

Owners and operators are encouraged to establish contact with their [regional Cybersecurity Advisors and Protective Security Advisors](#) to advance real-time coordination. These experts provide no-cost technical assistance, vulnerability scanning, risk assessments, and incident reporting pathways.

Entities should proactively share requests for information, suspicious network observations, scanning activity, or attempted credential compromises, even if these appear limited. Early notification enables federal partners to identify broader threat campaigns and provide tailored mitigation guidance. Coordination during anomalous activity will strengthen collective defense and accelerate protective measures within each sector.

CISA encourages critical infrastructure organizations to report suspicious or criminal activity related to this Alert at www.cisa.gov/report or via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).

Disclaimer

The information in this report is being provided “as is” for informational purposes only. CISA does not endorse any commercial entity, product, company, or service, including any entities, products, or services linked within this document. Any reference to specific commercial entities, products, processes, or services by service mark, trademark, manufacturer, or otherwise, does not constitute or imply endorsement, recommendation, or favoring by CISA.