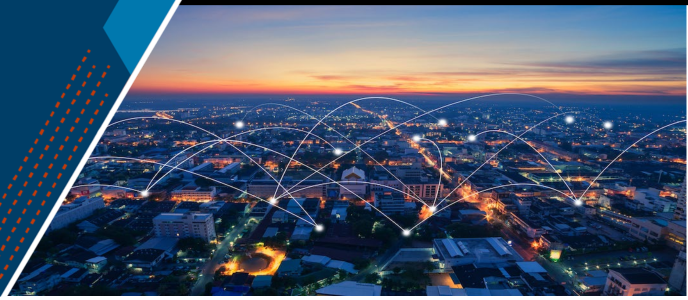

Iranian Cyber Actors May Target Vulnerable US Networks and Entities of Interest

Overview

The Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), the Department of Defense Cyber Crime Center (DC3), and the National Security Agency (NSA) (hereafter referred to as the authoring agencies) strongly urge organizations to remain vigilant for potential targeted cyber activity against U.S. critical infrastructure and other U.S. entities by Iranian-affiliated cyber 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 authoring agencies are continuing to monitor the situation and will release pertinent cyber threat and cyber defense information as it becomes available.

Threat Activity

Based on the current geopolitical environment, Iranian-affiliated cyber actors may target U.S. devices and networks for near-term cyber operations. Defense Industrial Base (DIB) companies, particularly those possessing holdings or relationships with Israeli research and defense firms, are at increased risk. Hacktivists and Iranian-government-affiliated actors routinely target poorly secured U.S. networks and internet-connected devices for disruptive cyberattacks.

Iranian-affiliated cyber actors and aligned hacktivist groups often exploit targets of opportunity based on the use of unpatched or outdated software with known Common Vulnerabilities and Exposures (CVEs) or the use of default or common passwords on internet-connected accounts and devices. (**Note:** See CISA's Known Exploited Vulnerabilities Catalog for more information on vulnerabilities that have been exploited in the wild). These malicious cyber actors commonly use techniques such as automated password guessing, cracking password hashes using online resources, and inputting default manufacturer passwords. When specifically targeting operational technology (OT), these malicious cyber actors also use system engineering and diagnostic tools to target entities such as engineering and operator devices, performance and security systems, and vendor and third-party maintenance and monitoring systems.

Over the past several months, Iranian-aligned hacktivists have increasingly conducted website defacements and leaks of sensitive information exfiltrated from victims. These hacktivists are likely to significantly increase distributed denial of service (DDoS) campaigns against U.S. and Israeli websites due to recent events.

Iranian-affiliated cyber actors may also conduct ransomware attacks in collaboration with other cybercriminal groups. These actors have been observed working directly with ransomware affiliates to conduct encryption operations, as well as steal sensitive information from these networks and leaking it online.

This document is marked TLP:CLEAR. Disclosure is not limited. Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be distributed without restriction. For more information on the Traffic Light Protocol, see cisa.gov/tlp.

Previous Cyber Campaigns

Between November 2023 and January 2024, during the Israel-Hamas conflict, Iranian Islamic Revolutionary Guard Corps (IRGC)-affiliated cyber actors actively targeted and compromised Israeli-made programmable logic controllers (PLCs) and human machine interfaces (HMIs). This global campaign included dozens of U.S. victims in the water and wastewater, energy, food and beverage manufacturing, and healthcare and public health sectors. The actors leveraged public internet-connected industrial control systems (ICSs) that used factory-default passwords, or no passwords, and default Transmission Control Protocol (TCP) ports.

Following the onset of the Israel-Hamas conflict, Iranian-affiliated cyber actors conducted several hack-and-leak operations to protest the conflict in Gaza. This campaign combined hacking and theft of data with information operations (e.g., online amplification through social media or threats and harassment using direct messaging). These operations resulted in financial losses and reputational damage for victims. The purpose of these campaigns was to undermine public confidence in the security of victim networks and data, as well as embarrass targeted companies and countries. While hacktivists primarily targeted Israeli companies, one instance involved a U.S. internet protocol television (IPTV) company.

Mitigations

The authoring agencies strongly urge critical infrastructure asset owners and operators to implement the following mitigations to harden their cyber defenses against malicious actors.

- Identify and disconnect OT and ICS assets from the public internet.
  - Focus on remote access technologies such as virtual network computing (VNC), remote desktop protocol (RDP), Secure Shell Protocol (SSH) and web management interfaces (as part of an HMI, virtual private network [VPN], or otherwise).
  - Adopt a deny-by-default allowlist policy to prevent unauthorized access if an asset's remote access cannot be removed.
- Ensure devices and accounts are protected with strong, unique passwords (if not using multifactor authentication [MFA]) and immediately replace weak or default passwords.
  - Use Role-Based Access Controls (RBAC) and conditional access policies for cloud service or managed service providers.
- Implement phishing-resistant MFA for accessing OT networks from any other network.
  - Consider strategically requiring MFA for changes to high value controllers that are difficult to replace or could be significantly impacted if compromised.
- Apply the manufacturer's latest software patches for internet-facing systems to ensure protection against known vulnerabilities.
- Prioritize monitoring user access logs for remote access to the OT network and for implementation of any firmware or configuration changes.
- To reduce the impact of a successful intrusion, establish OT processes that prevent unauthorized changes, loss of view, or loss of control (e.g., PLCs in run mode rather than program mode, hardware or software interlocks, safety systems, and redundant sensors).
- Ensure business continuity and incident response plans are in place for a swift recovery, including implementing full system and data backups to facilitate any recovery efforts.

  - Review incident response plans and update as needed.
  - Rehearse critical system recovery efforts and related actions, and update incident response plans based on results.
- Consider how exfiltrated data, such as leaked credentials, could be leveraged to conduct further malicious activity against your network, and ensure security mechanisms are in place to reduce the impact of a potential leak.

Resources

The authoring agencies, in collaboration with U.S. and foreign government partners, have previously released advisories describing high-level cyber tactics employed by Iranian-affiliated cyber actors and general guidance to harden systems and networks against this threat. The authoring agencies strongly recommend critical infrastructure organizations and other entities review the following resources for more information on this cyber threat and additional mitigations. The list below also incorporates physical security resources.

- For an overview of the Iranian threat, refer to CISA's Iran Threat Overview and Advisories and the FBI's The Iran Threat webpages.
- For a list of cybersecurity advisories attributed to Iranian state-sponsored cyber actors, refer to CISA's Iran State-Sponsored Cyber Threat: Advisories webpage.
- Refer to the following FBI resources for additional Iranian-attributed joint products:
  - Joint cybersecurity advisory: New Tradecraft of Iranian Cyber Group Aria Sepehr Ayandehsazan aka Emennet Pasargad.
  - Joint cybersecurity advisory: Iranian Cyber Actors Targeting Personal Accounts to Support Operations.
  - Private industry notification (PIN): Iranian Cyber Group Emennet Pasargad Conducting Hack-and-Leak Operations Using False-Flag Personas.
- For Unitronics PLC-specific background and mitigations, refer to the joint cybersecurity advisory IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including US Water and Wastewater Systems Facilities.
- For more information on CyberAv3ngers, refer to the Department of State's Reward for Justice: CyberAv3ngers.
- For more information on techniques used to target OT and ICS, refer to the joint cybersecurity advisory Control System Defense: Know the Opponent.
- For more information on reducing the risk of cyber threats to OT, refer to the joint fact sheet Primary Mitigations to Reduce Cyber Threats to Operational Technology.
- For more information on defending against DDoS attacks, refer to the joint guide Understanding and Responding to DDoS Attacks.
- For more information on CVEs, refer to the joint advisory 2023 Top Routinely Exploited Vulnerabilities.
- For more information on improving cybersecurity and physical defenses, refer to CISA Insights: Increased Geopolitical Tensions and Threats.

- For more information on protecting physical environments, refer to CISA's Physical Security – Preventative and Protective Strategies webpage.

Contact Information

The authoring agencies recommend U.S. organizations report suspicious or criminal activity related to information in this fact sheet.

- **CISA:** Contact CISA via CISA's 24/7 Operations Center (report@cisa.gov or 888-282-0870).
  - When available, please include the following information regarding the incident: date, time, and location of the incident; type of activity; number of people affected; type of equipment used for the activity; the name of the submitting company or organization; and a designated point of contact.
  - For more information on reporting a cyber incident, refer to CISA's Voluntary Cyber Incident Reporting webpage.
- **FBI:** If you believe you have been the victim of Iranian cyber activity as described above, contact your relevant security officials and the FBI. The FBI requests victims report any incident to your local FBI Field Office or the Internet Crime Complaint Center (IC3) at www.ic3.gov. Include as much detailed information about the incident as possible.
- **NSA:** For NSA cybersecurity guidance inquiries, contact CybersecurityReports@nsa.gov.
- **DC3:** For DIB inquiries and cybersecurity services, contact DC3.DCISE@us.af.mil. For media inquiries or the press desk, contact DC3.Information@us.af.mil.

Disclaimer

The information in this report is being provided "as is" for informational purposes only. The authoring agencies do 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 favor by the authoring agencies.