CAA-2026-0009 Iran-Linked Cyber Activity and Relevance to Alberta Organizations

Summary

On 28 February 2026, the United States (U.S.) and the State of Israel (Israel) launched military strikes against the Islamic Republic of Iran (Iran). Canadian organizations, especially those with operations in the Middle East, should review their cybersecurity posture and remain vigilant to threats posed by Iranian-aligned cyber threat actors.

Details

On 28 February 2026, the Prime Minister of Canada released a statement expressing support for U.S. military actions taken against Iran and Israel's right to defend itself.[1] The Canadian Department of National Defence also stated that the Canadian Armed Forces members were not involved in the U.S. military operation, nor its planning.[2]

The Canadian Centre for Cyber Security (CCCS) cautions Canadian organizations that Iran and Iran-aligned threat actors may respond to the joint U.S.-Israeli military strikes with cyber-enabled operations.[3] Iranian-aligned actors are more likely to conduct cyber-attacks, disinformation campaigns, and disruptive attacks against Canadian critical infrastructure operators and organizations with operations or supply-chain ties in the Middle East.

CCCS characterizes Iranian cyber activity into the following groups:

- Social engineering and spear phishing attacks targeting both government and private-sector networks.
- Exploitation of known vulnerabilities to gain initial access to support data exfiltration, ransomware, or extortion operations.
- Disruptive attacks such as website defacements, Distributed Denial of Service (DDoS) attacks, and deploying wiper malware.

Observed Hacktivist Activity

The ongoing U.S.-Israel-Iran conflict has already led to an observable increase in hacktivist activity from Iranian-aligned groups. On 2 March 2026, Palo Alto's Unit 42 researchers identified a surge in activity from pro-Iranian, pro-Russian, and pro-Palestinian hacktivist groups. These hacktivist groups have claimed responsibility for a wide range of disruptive operations against organizations primarily located in the Middle East.[4] These hacktivist groups are likely to target organizations they consider involved in the Iran conflict using DDoS attacks, website defacements, and hack-and-leak campaigns.[5] [6]

[1] https://www.pm.gc.ca/en/news/statements/2026/02/28/statement-prime-minister-carney-and-minister-anand-situation-middle-east
[2] https://www.cbc.ca/news/politics/iran-air-strikes-canada-israel-war-9.7110268
[3] https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-response-usisrael-strikes-february-2026
[4] https://unit42.paloaltonetworks.com/iranian-cyberattacks-2026/
[5] https://blog.checkpoint.com/research/what-defenders-need-to-know-about-irans-cyber-capabilities/
[6] https://www.reuters.com/business/media-telecom/hackers-hit-iranian-apps-websites-after-us-israeli-strikes-2026-03-01/

Alberta-based organizations with operations in the Middle East—especially in the energy, oil, and gas sectors—are at a higher risk of facing disruptions. Such organizations should exercise vigilance and plan accordingly for operational disruptions in the Middle East.

Cyber Activity Following Twelve-Day War

Following the June 2025 conflict between Israel, the U.S., and Iran—known as the Twelve-Day War, Iran-aligned hacktivist groups primarily conducted DDoS attacks, website defacements, and data exfiltration attacks.[7]

During the same period, an Iranian state-affiliated actor also conducted a conflict-themed phishing attack to deploy malware.[8] The majority of attacks were targeted Israeli and U.S. critical infrastructure.[9][10] At the time, CCCS noted a heightened risk for all organizations due to increased opportunistic activity seeking to undermine Israel, U.S., and their allies.[11]

Assessment

CyberAlberta Threat Intelligence assesses that if Iran-aligned cyber threat actors target Canadian organizations they would likely prioritize those with operations in the Middle East. Pro-Iranian hacktivist groups may also target Canadian organizations with disruptive attacks in response to Canada's support for U.S.-Israeli military actions.

Recommendations

Alberta-based organizations should review their cybersecurity posture and consider the following:

- Strengthen identity and access controls by implementing phishing-resistant multi-factor authentication (MFA), especially for privileged and administrative accounts.[12]
- Ensure public-facing devices are fully inventoried, with internet access removed if no longer required.
- Apply the latest patches for all assets hosted on these devices and confirm that default credentials have been removed, with particular attention to Industrial Control Systems (ICS) such as Programmable Logic Controllers (PLCs).
- Review and apply CCCS cybersecurity hygiene best practices.[13]
- Subscribe to the National Cyber Threat Notification System (NCTNS) from CCCS to receive timely alerts on cyber threats relevant to your organization.
- Report suspected malicious cyber activity to CyberAlberta[14] and the CCCS.[15]

[7] https://unit42.paloaltonetworks.com/iranian-cyberattacks-2025/
[8] https://securityscorecard.com/blog/from-the-depths-of-the-shadows-irgc-and-hacker-collectives-of-the-12-day-war/
[9] https://cyble.com/blog/hacktivists-launch-ddos-attacks-at-us-iran-bombings/
[10] https://outpost24.com/blog/hacktivist-cyber-operations-iran-israel/
[11] https://www.cyber.gc.ca/en/guidance/cyber-threat-bulletin-iranian-cyber-threat-canada-israel-iran-conflict
[12] https://www.cyber.gc.ca/en/guidance/defending-against-adversary-middle-threats-phishing-resistant-multi-factor-authentication-itsm30031
[13] https://www.cyber.gc.ca/en/guidance/cyber-security-hygiene-best-practices-your-organization-itsap10102
[14] https://cyberalberta.ca/report-a-cyber-issue
[15] https://www.cyber.gc.ca/en/incident-management