Iranian APT Activity Escalates Amid Geopolitical Conflict: Recommendations for Critical Infrastructure Defenders

Tracking ID#: PCS-03-0426

Date: 04-03-2026

Disclaimer: This is a shared security advisory service; hence, it can be communicated to a single dedicated point of contact. We would highly appreciate it if you assigned them to your organisation's concerned asset/technology owner. Please use it as applicable to your environment

Date: 04-03-2026

Summary:

Nozomi Networks Labs is tracking a big rise in cyber activity linked to the Iranian government after open conflict began involving Iran, Israel, and the United States. This includes Operation Lion's Roar coordinated military strikes on Iranian military and nuclear sites and the retaliations that followed. The conflict has moved beyond physical attacks into cyberspace. Iranian threat groups are using their advanced persistent threat (APT) skills to target foreign networks and industrial control systems as part of their wider goals. Analysis of anonymous data from the last two weeks shows a steady increase in alerts related to Iran-linked APTs. The Manufacturing and Transportation sectors are the most targeted. Key threat groups include: MuddyWater (APT34/OilRig/Seedworm), a group linked to MOIS that carries out cyber spying through spear-phishing and using existing system tools; OilRig (APT34/Helix Kitten), which focuses on government, financial, and energy sectors using custom backdoors and web shells; APT33 (Elfin/Refined Kitten), targeting aerospace, aviation, energy, and manufacturing through spear-phishing and password spraying; and UNC1549 (also known as CURIUM/Tortoise Shell/Crimson Sandstorm), active in defense, aerospace, telecommunications, and government sectors. An analysis of Middle Eastern organizations' security shows a worrying situation: 61% of found vulnerabilities are HIGH or CRITICAL (CVSS), which is twice the global average of 48%. Also, 8% of vulnerabilities have EPSS scores over 1%, double the global average of 4%. The main MITRE ATT&CK techniques seen (default credential abuse, valid account use, brute force, scanning) show attackers are in the early stages exploring systems, finding important assets, and setting up access. This period of reconnaissance is a key chance for defenders to stop attacks before they move on to privilege escalation, stealing data, or causing damage.

Target:

Applicable to all users.

Mitigation Recommendations:

Recommended to block the IOCs listed below.

S.No	Indicators of Compromise (IOCs)	Type
1	37[.]1[.]213[.]152	IP
2	184[.]75[.]210[.]206	

References:

- Iranian APT Activity During Geopolitical Escalation: Recommendations for Nozomi Customers and Critical Infrastructure Owners