RSM Defense

Reversing the adversary's advantage

Threat Alert - Ongoing Campaign - Iran-Linked Cyber Campaign Exploits Internet-Exposed PLCs to Disrupt US Critical Infrastructure

TLDR/BLUF:

Iran-affiliated cyber actors are actively exploiting internet-exposed programmable logic controllers (PLCs), particularly Rockwell Automation/Allen-Bradley devices, across US critical infrastructure sectors. This campaign has resulted in confirmed operational disruptions, manipulation of HMI/SCADA data, and theft of PLC project files, with financial losses reported in water, energy, and government facilities. The attacks reflect an evolution in Iranian operational technology (OT) targeting, shifting from defacement to direct process interference, and are enabled primarily by poor network architecture and exposed OT assets rather than advanced exploitation techniques. The threat is heightened during periods of geopolitical tension, increasing the risk of real-world impact.

RSM Defense is continuing to monitor the ongoing Iranian conflict and conducting threat hunts and analysis within client environments on the evolving threats and reported IOCs/TTPs. Technical details and recommendations for how to protect organizations against these campaigns can be seen below.

Incident/Report Details:

- **Date of Incident/Report:** April 14, 2026
- **Industries Affected:** Critical Infrastructure (including Water, Energy, Oil & Natural Gas, Government Services and Facilities)
- **Severity:** High (confirmed operational disruption and financial loss)
- **Affected Software:** Rockwell Automation/Allen-Bradley PLCs; likely extends to other internet-exposed industrial control systems
- **Regions Affected:** United States

Incident Description:

Iran-linked threat actors are conducting a coordinated campaign targeting US critical infrastructure by exploiting internet-facing PLCs, with a focus on Rockwell Automation/Allen-Bradley devices. The attacks have resulted in diminished PLC functionality, unauthorized manipulation of HMI/SCADA display data, and theft of project configuration files. These actions have caused operational disruptions and financial losses in sectors such as water, energy, and government facilities.

The campaign is characterized by its reliance on accessible attack surfaces specifically, OT assets that are directly exposed to the internet, rather than sophisticated intrusion techniques. Iranian groups, including CyberAv3ngers, Static Kitten (MuddyWater), Refined Kitten (APT33), Helix Kitten (APT34), and Banished Kitten, are implicated. These groups use a combination of direct OT disruption, espionage, and access operations to achieve rapid operational effects and maintain plausible deniability.

Recent incidents include disruptions at a US-based medical device manufacturer and ongoing access operations targeting US financial institutions, transportation infrastructure, and defense supply chains. The campaign marks a shift from previous Iranian operations that focused on defacement and signaling, moving toward direct interference with industrial processes and data, thereby increasing the likelihood of real-world impact, especially during periods of heightened geopolitical tension.

Technical Details:

Technical Campaign Details:

- **Primary Attack Vector:** Exploitation of internet-exposed PLCs, especially Rockwell Automation/Allen-Bradley devices.
- **Observed Impacts:** Diminished PLC functionality, unauthorized HMI/SCADA data manipulation, theft of project configuration files, operational disruption, and financial loss.
- **Attack Surface:** Reliance on accessible, poorly secured OT assets rather than advanced exploits.
- **Protocols/Ports Monitored:** EtherNet/IP (44818), 2222, 102, 502 (Modbus).
- **Recent Escalations:** Disruption at a US medical device manufacturer (Handala persona), MuddyWater targeting US financial, transportation, and defense sectors.
- **Evolution:** Shift from defacement to direct process interference, increasing real-world operational risk.
- **Detection Challenges:** Use of commodity access techniques and early-stage tooling with low detection rates across traditional security engines.

Layered Campaign Models:

- **Access Layer:** MuddyWater, OilRig establish footholds in enterprise/infrastructure-adjacent environments.
- **Targeting Layer:** APT33 and similar actors focus on strategic industries (energy, aerospace).

- **Disruption Layer:** CyberAv3ngers and similar groups directly target OT systems for immediate operational impact.

Threat Actor	Brief Summary	TTPs	Targeted Industries/Regions
CyberAv3ngers	Iranian group active since 2023, likely operating under/with IRGC Cyber Electronic Command. Focuses on direct OT disruption, especially PLCs in water and wastewater. Known for leveraging exposed infrastructure and shifting from defacement to operational disruption.	- Exploits internet-exposed PLCs and industrial control devices - Manipulates HMI/SCADA data and system outputs - Disrupts water and energy systems - Uses public personas for psychological impact - Leverages weak/default configurations	- Water and wastewater systems - Energy and utilities - Government-operated infrastructure - Industrial environments using exposed PLCs - Regions: US, Israel, allied infrastructure
MuddyWater (Static Kitten)	Active since at least 2017, operates under Iran's MOIS. Focuses on espionage and access operations, enabling broader campaigns. Not primarily OT-disruptive but establishes footholds for future disruption.	- Spearphishing and credential harvesting - PowerShell and living-off-the-land techniques - Custom and commodity backdoors - Persistence via legitimate admin tools - Reconnaissance and lateral movement	- Government/public sector - Energy and oil & natural gas (ONG) - Telecommunications - Financial institutions - Defense/supply chain - Regions: Middle East, US, Europe, Asia, Africa
APT33 (Refined Kitten)	Active since at least 2013, associated	- Spearphishing and credential harvesting - Password spraying	- Energy/utilities - Aerospace/aviation - Defense contractors

	with Iranian state interests. Focuses on strategic industries (energy, aerospace, defense) for disruption and intelligence. Capable of destructive malware deployment.	- Malware for persistence/destruction - Targets enterprise environments supporting industrial ops - Reconnaissance and long-term access	- Industrial/manufacturing - Regions: US, Middle East, Europe, Asia
APT34 (Helix Kitten/OilRig)	Active since at least 2014, operates under MOIS. Persistent espionage actor, focuses on long-term access and intelligence collection, especially in energy sector and infrastructure-adjacent organizations.	- Spearphishing and web shell deployment - Credential theft and privilege escalation - Custom malware and legitimate tools for persistence - Lateral movement - Intelligence collection	- Energy sector - Government entities - Defense/intelligence organizations - Telecommunications/infrastructure-adjacent - Regions: Middle East, US, Europe, strategic targets
Banished Kitten (Dune, Void Manticore, Red Sandstorm, Storm-0842)	Active since at least 2008, operates under/with MOIS. Evolved from espionage to hybrid disruption, data leakage, and influence campaigns. Uses front personas for plausible deniability and psychological impact.	- Targeted intrusions via spearphishing, credential harvesting, exploiting exposed services - Destructive ops (data wiping, system disruption) - Data exfiltration/leakage - Influence personas (Handala, Homeland Justice) - Persistence via remote access, tunneling, admin abuse	- Government/public sector - Critical infrastructure/industrial environments - Private sector (healthcare, manufacturing) - Media/dissidents - Regions: Middle East, US, Europe, allied nations

Remediation & Recommendations:

RSM Defense is continuing to monitor the ongoing Iranian conflict and conducting threat hunts and analysis within client environments on the evolving threats and reported IOCs/TTPs. Recommendations for how to protect organizations against these campaigns can be seen below.

- **Remove Internet Exposure:** Immediately disconnect PLCs and other industrial control systems from direct internet access.
- **Monitor Industrial Protocols:** Increase monitoring for suspicious activity on industrial protocols and ports, including EtherNet/IP (44818), 2222, 102, and Modbus (502).
- **Harden Configurations:** Change default credentials, disable unused services, and apply network segmentation to limit lateral movement.
- **Patch and Update:** Ensure all OT and IT systems are up to date with the latest security patches and firmware updates.
- **Incident Response Planning:** Develop and regularly test incident response plans specific to OT environments, including procedures for rapid isolation and recovery.
- **Threat Intelligence Integration:** Leverage multi-engine malware analysis platforms to detect low-consensus or emerging threats that may evade traditional security tools.
- **User Awareness:** Train staff on spearphishing and credential harvesting tactics commonly used by Iranian threat actors.
- **Collaboration:** Engage with sector-specific Information Sharing and Analysis Centers (ISACs) and follow guidance from US government advisories (e.g., CISA AA26-097A).

By addressing architectural vulnerabilities and improving detection and response capabilities, organizations can significantly reduce the risk of successful exploitation by Iranian-linked threat actors.

Sources:

1. RSM Internal Sources
2. PolySwarm Threat Bulletin_Iran-Linked PLC Exploitation Expands Across US Critical Infrastructure_04-14-26.pdf

SILOBREAKER

Privacy Policy and Terms of Use