**Cyber-Influence Operation Analysis:**

**Background, Documentation, and Modelling of Cyber and Disinformation Components.**

# Iranian Influence in Israel-Hamas Conflict

## Summary

Iranian threat actor, CyberAveng3rs, targeted Israeli PLCs (Programmable Logic Computer) in the water, shipping, and distribution sectors. The Cyber Aveng3rs Telegram channel displayed claims of cyberattacks against Israel. Some claims were shown to be fabricated whilst others were legitimate. In a specific incident, CyberAveng3rs breached a water control display on a Unitronics Vision Series PLC at a US water facility. The PLC was defaced, displaying an image containing text that read “You have been hacked, down with Israel. Every equipment ‘made in Israel’ is Cyberav3ngers legal target.” The PLCs were accessed using default passwords. According to OpenAI, members of CyberAv3ngers used ChatGPT to gain information about PLCs and their default passwords. The group behind the attack was identified by Microsoft as Storm-0784.

## Timeline and Context

September 13 – October 30 2023

* CyberAv3ngers Telegram channel displays claims of cyberattacks against Israel
* Displays both legitimate and false claims
* Targeting Israeli PLCS in the water, energy, shipping & distribution sectors

From November 22, 2023

* IRGC threat actors accessed water utility control systems
* “US based WWS facilities that operate Unitronics Vision Series PLCs with an HMI”
* PLC = programmable logic controller
* Software previously did not require users to change the default passwords
* Likely compromised by compromising internet-accessible devices with default passwords
* Displaying message “You have been hacked, down with Israel. Every equipment ‘made in Israel’ is Cyberav3ngers legal target.”

## Frameworks

Description and Justification of the techniques can be found in the corresponding intermediary table document.

### ATT&CK Framework

* **TA0043: Reconnaissance** 
  + T1592.001:Gather Victim Host Information: Hardware
  + T1592.002: Gather Victim Host Information: Software
  + T1596: Search Open Technical Databases
  + T1589.001: Gather Victim Identity Information: Credentials
* **TA0001: Initial Access**
  + T1133: External Remote Services
  + TA0001: Valid Accounts: Default Accounts
* **TA0042: Resource Development**
  + T1650: Acquire Access
* **TA0011: Command and Control**
  + T1659: Content Injection
* **TA0040: Impact**
  + T1491.001: Defacement: Internal Defacement

### DISARM Framework

* **PLAN**:
  + TA01: Plan Strategy
    - T0073: Determine Target Audiences
    - T0074: Determine Strategic Ends
  + TA02: Plan Objectives
    - T0002: Facilitate State Propaganda
    - T0066: Degrade Adversary
  + TA13: Target Audience Analysis
    - T0081: Identify Social and Technical Vulnerabilities
* **PREPARE**:
  + TA14: Develop Narratives
    - T0068: Respond to Breaking News Event or Active Crisis
    - T0082: Develop New Narratives
  + TA06: Develop content
    - T0085: Develop Text-based Content
    - T0086: Develop Image-based Content
    - T0023: Distort facts
    - T0084: Reuse Existing Content
  + TA16: Establish Legitimacy
    - T0011: Compromise legitimate accounts
  + TA07: Select Channels and Affordances
    - T0043.001: Use Encrypted Chat Apps
    - T0043: Chat Apps
* **EXECUTE**:
  + TA09: Deliver Content
    - T0117: Attract Traditional Media
  + TA11: Persist in the Information Environment
    - T0128.001: Use Pseudonyms

## Resources

This includes resources used to produce a timeline, technical information, tactics, techniques, and procedures used in the operation. It can also include any relevant resources that support modelling decisions such as technical methods for cyber components or societal/psychological context for influence components.

<https://blogs.microsoft.com/on-the-issues/2024/02/06/iran-accelerates-cyber-ops-against-israel/>

<https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/iran-surges-cyber-enabled-influence-operations-in-support-of-hamas>

<https://www.politico.com/news/2023/11/28/federal-government-investigating-multiple-hacks-of-us-water-utilities-00128977>

<https://blog.google/technology/safety-security/tool-of-first-resort-israel-hamas-war-in-cyber/>

<https://services.google.com/fh/files/misc/tool-of-first-resort-israel-hamas-war-cyber.pdf>

<https://www.cisa.gov/sites/default/files/2023-12/aa23-335a-irgc-affiliated-cyber-actors-exploit-plcs-in-multiple-sectors-1.pdf>

<https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a>

<https://www.cyber.gov.au/about-us/view-all-content/alerts-and-advisories/exploitation-unitronics-programmable-logic-controllers-plcs>

<https://securelist.com/a-hack-in-hand-is-worth-two-in-the-bush/110794/>

<https://cdn.openai.com/threat-intelligence-reports/influence-and-cyber-operations-an-update_October-2024.pdf>

<https://cdn-dynmedia-1.microsoft.com/is/content/microsoftcorp/microsoft/final/en-us/microsoft-brand/documents/Microsoft%20Digital%20Defense%20Report%202024%20%281%29.pdf>