<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.theguardian.com/technology/2024/feb/08/iran-backed-hackers-interrupt-uae-tv-streaming-services-with-deepfake-news>

<https://www.khaleejtimes.com/uae/uae-cyberattack-disrupts-tv-services-rattles-some-residents-with-graphic-content-from-gaza>

<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/>

**tv channel hacking UAE**

* Interrupted broadcast
* AI generated video which discussed the Israel-Hamas conflict

**Cyber Avengers target Israeli PLCS to promote Hamas**

**Summary**

* Cyber Av3ngers breached control panel for water utilities, disabling it
* Displaying a message “you have been hacked, down with israel, every equipment made in Israel is cyber-avengers legal target’

**Timeline**

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

October 13 2023

* Soldiers of Solomon (linked to CyberAv3ngers) claim to have compromised > 50 servers, security cameras, etc in Israel
* Most claims proven false
* Claimed to have used ransomware “Crucio”

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.”

Components : defacement, credential access, brute force, legitimate & false claims, telegram network,

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Telegram channel** | | | |
| Displaying claims of cyberattacks against Israel in the channel | DISARM: Respond to Breaking News Event or Active Crisis |  |  |
| DISARM: Use Encrypted Chat Apps |  |  |
| DISARM: Chat apps |  |  |
| False claims | DISARM: Develop New Narratives |  |  |
| DISARM: Distort facts |  |  |
| DISARM: Reuse Existing  Content |  |  |
| Legitimate claims |  |  |  |
| Targeting PLCS (Programmable logic controllers) |  |  |  |
| **Access water utility control system** | | | |
| Compromising internet-accessible devices with default passwords | DISARM: Identify Social and Technical Vulnerabilities | Technical vulnerabilities in the PLC systems would have been identified to later exploit. |  |
| ATT&CK: Gather Victim Host Information: Hardware | To gain access to the PLC, information on the system’s hardware would have been gathered. |  |
| ATT&CK: Gather Victim Host Information: Software | Older versions of the PLC VisiLogic software did not require users to change default passwords. |  |
| ATT&CK: Gather Victim Identity Information: Credentials | Default passwords were found to later use them to access the PLC. |  |
| ATT&CK: Search Open Technical Databases \* | To identify the default passwords, it is likely that the threat actor would have searched technical databases. |  |
| ATT&CK: Acquire Access | After using the default password, they gained access to the PLCS. |  |
| ATT&CK: Compromise Infrastructure \* | The PLC infrastructure was compromised. |  |
| ATT&CK: External Remote Services \* | The PLCs were accessed remotely. |  |
| ATT&CK: Valid Accounts: Default Accounts | The PLCs were accessed using default passwords for default accounts. |  |
| DISARM: Compromise legitimate accounts | Default accounts are legitimate so this technique is applicable. |  |
| Creation of image and narrative used in defacement | DISARM: Facilitate State Propaganda |  |  |
| DISARM: Degrade Adversary |  |  |
| DISARM: Develop Image-based Content |  |  |
| DISARM: Develop Text-based Content |  |  |
| Identifying as CyberAv3ngers | DISARM: Use  Pseudonyms |  |  |
| Defacement of the PLCs | ATT&CK: Content Injection |  |  |
| ATT&CK: Defacement: Internal Defacement |  |  |
| ATT&CK: Service Stop \* |  |  |
| DISARM: Attract Traditional Media |  |  |

\*Can also add the broadcasting attack and soldiers of Solomon if more needed