**CyberAv3ngers – Iranian Influence in Israel-Hamas Conflict**

|  |  |  |  |
| --- | --- | --- | --- |
| Event | Technique | Comments | Verified |
| **Telegram channel** | | | |
| Displaying claims of cyberattacks against Israel in the channel | DISARM: Respond to Breaking News Event or Active Crisis | Claims of cyberattacks against Israel were posted in response to the ongoing Israel-Hamas conflict |  |
| DISARM: Use Encrypted Chat Apps | CyberAv3ngers used Telegram, an encrypted chat app to display claims of cyberattacks against Israel. |  |
| DISARM: Chat apps |
| False claims | DISARM: Develop New Narratives | CyberAv3ngers used content from past cyberattacks and other groups to claim they had recently performed cyberattacks. |  |
| DISARM: Distort facts |
| DISARM: Reuse Existing  Content |
| Legitimate claims |  | Not present. Could not identify a technique to reflect the use of sharing legitimate claims. |  |
| **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 | The message in the defacement directly displays “You have been hacked, down with Israel. Every equipment ‘made in Israel’ is Cyberav3ngers legal target.” |  |
| DISARM: Degrade Adversary |  |
| DISARM: Develop Image-based Content | The image for the defacement needed to be developed, which was also largely text based. |  |
| DISARM: Develop Text-based Content |
| Identifying as CyberAv3ngers | DISARM: Use  Pseudonyms | The threat actor group identified themselves within the defacement as CyberAv3ngers. |  |
| Defacement of the PLCs | ATT&CK: Content Injection | The content used for the defacement was displayed on the PLCs. In doing so, the PLCs became inoperable temporarily. |  |
| ATT&CK: Defacement: Internal Defacement |
| ATT&CK: Service Stop \* |
| DISARM: Attract Traditional Media | Through defacing these devices, it is likely that CyberAv3ngers aimed to garner the attention of traditional media. |  |
| **Other activity (before or after cyber-attacks used, or just occurring generally)** | | | |
| Before | DISARM: Determine Target Audiences | Before conducting their operation, CyberAv3ngers would have determined their target audiences and their strategic ends. |  |
| DISARM: Determine Strategic Ends |
| After |  | Not present  There was no evidence found to suggest that CyberAv3ngers conducted any post-operation analysis. It is probable that this may have occurred, so could be added with the appropriate confidence level. |  |