CyberAv3ngers – Rewards For Justice

Archived: 2026-04-05 18:03:57 UTC

Rewards for Justice is offering a reward of up to $10 million for information leading to the identification or location of any person who, while acting at the direction or under the control of a foreign government, participates in malicious cyber activities against U.S. critical infrastructure in violation of the Computer Fraud and Abuse Act (CFAA).

Hamid Homayunfal, Hamid Reza Lashgarian, Mahdi Lashgarian, Milad Mansuri, Mohammad Bagher Shirinkar, and Mohammad Amin Saberian are Iranian security officials linked to malicious cyber activities of Iran's Islamic Revolutionary Guard Corps (IRGC) hacking groups.

Hamid Reza Lashgarian is the head of the IRGC's Cyber-Electronic Command (IRGC-CEC) and is also a commander in the IRGC-Qods Force, which is Iran's primary mechanism for cultivating and supporting terrorist groups abroad. He has been involved in various IRGC cyber and intelligence operations.

Hamid Homayunfal, Mahdi Lashgarian, Milad Mansuri, Mohammad Amin Saberian, and Mohammad Bagher Shirinkar are senior officials of the IRGC-CEC.

CyberAv3ngers, affiliated with the IRGC-CEC and Mahdi Lashgarian, utilized malware known as IOCONTROL to target worldwide industrial control system/supervisory control and data acquisition (ICS/SCADA) devices, including routers, PLCs, human machine interfaces (HMIs), firewalls, IP cameras, and Linux-based Internet of Things (IoT) and SCADA/Operational Technology platforms. IOCONTROL is a cyberweapon that has been used to attack vendors, including but not limited to Baicells, D-Link, Hikvision, Red Lion, Orpak, Phoenix Contact, Teltonika, Unitronics, and other civilian infrastructure in several countries worldwide.

CyberAv3ngers has targeted and compromised the Vision series of programmable logic controllers (PLCs) made by Israel-based Unitronics. The PLCs are used by the water and wastewater, energy, food and beverage, manufacturing, healthcare, and other industries, and may be re-branded as manufactured by other companies.

In October 2023, CyberAv3ngers actors claimed credit for cyberattacks against Israeli PLCs on their Telegram channel.

Since at least November 22, 2023, CyberAv3ngers actors have compromised the default credentials in these PLCs across the United States and left a message on the devices' digital screen stating, "You have been hacked, down with Israel. Every equipment 'made in Israel' is CyberAv3ngers legal target." The compromise of the device also may render it inoperative.

On February 2, 2024, the U.S. Department of the Treasury announced sanctions against the six IRGC-CEC officials for their malicious cyber activities. Hamid Homayunfal, Hamid Reza Lashgarian, Mahdi Lashgarian, Milad Mansuri, Mohammad Amin Saberian, and Mohammad Bagher Shirinkar were named as Specially Designated Nationals pursuant to the counterterrorism authority Executive Order (E.O.) 13224, as amended for being leaders or officials of the IRGC-CEC.

As a result of these designations, all property and interests in property of these IRGC-CEC officials that are in the United States or in the possession or control of U.S. persons are blocked. The designations generally prohibit all transactions by U.S. persons or within (or transiting) the United States that involve any property or interests in property of designated or otherwise blocked persons.

Anyone with information on CyberAv3ngers malicious cyberactivity, associated individuals, or entities should contact Rewards for Justice via the Tor-based tips-reporting channel at: he5dybnt7sr6cm32xt77pazmtm65flqy6irivtflruqfc5ep7eiodiad.onion (Tor browser required)
