US offering $10 million for info on Iranian hackers behind IOControl malware

By Jonathan Greig

Published: 2025-06-16 · Archived: 2026-04-06 03:31:31 UTC

The U.S. State Department said they were seeking information on Iranian hackers who they accused of targeting critical infrastructure using a strain of malware deployed against industrial control systems.

U.S. officials are offering up to $10 million for details on a hacker affiliated with the group called CyberAv3ngers that gained prominence in 2023 and 2024 for a string of cyberattacks on U.S. and Israeli water utilities.

Law enforcement agencies eventually tied CyberAv3ngers to Iran's Islamic Revolutionary Guard Corps Cyber-Electronic Command, and in August offered a reward for information on at least six Iranian government hackers allegedly behind the effort and placing sanctions on the men.

On Thursday, the State Department issued a new reward centered around an online persona known as Mr. Soul or Mr. Soll. The notice said CyberAv3ngers is associated with the persona and "has launched a series of malicious cyber activities against U.S. critical infrastructure on behalf of Iran's Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC)."

"CyberAv3ngers actors have utilized malware known as IOCONTROL to target [Industrial Control Systems/Supervisory Control and Data Acquisition (ICS/SCADA)] devices used by critical infrastructure sectors in the United States and worldwide," the State Department said.

The State Department and Cybersecurity and Infrastructure Security Agency did not respond to requests for information about the most recent CyberAv3ngers attacks.

Members of CyberAv3ngers have boasted on Telegram of their attacks and compromises using IOControl.

IOControl is a strain of malware spotlighted by government officials in December 2024 that multiple cybersecurity firms said was being used by Iranian actors to attack Israel- and U.S.-based devices. Experts at Claroty said the malware was used to attack cameras, routers, firewalls and other industrial technology created by popular vendors like Unitronics, D-Link, Hikvision, Baicells and more.

Claroty incident responders analyzed a sample of the malware taken from a popular gas station management system that was allegedly compromised by CyberAv3ngers.

The malware allows hackers to remotely control infected devices, move laterally within a victim's system and more. Cybersecurity firm Armis said the malware was first seen using other names over a year ago.

The State Department reward was posted amid a widening military conflict between Israel and Iran. On Friday, Israeli missile strikes killed hundreds of Iranian citizens including several military leaders and nuclear scientists.

Iran has responded by firing hundreds of rockets at Israel, killing dozens in Tel Aviv and other cities.

John Hultquist, chief analyst at Google Threat Intelligence Group, warned that Iranian cyber threat actors would likely “rededicate themselves” to attacks on Israel in light of the recent conflict.

“Iranian cyber activity in Israel is already persistent and aggressive, and has been for several years. Iranian cyber activity has not been as extensive outside of the Middle East but could shift in light of the military actions,” he said.

“Targets in the United States could be reprioritized for action by Iran’s cyber threat capability. Iranian cyber espionage activity already targets the U.S. government, military, and political set, but new activity may threaten privately owned critical infrastructure, or even private individuals.”

No previous article

No new articles

Jonathan Greig

is a Breaking News Reporter at Recorded Future News. Jonathan has worked across the globe as a journalist since 2014. Before moving back to New York City, he worked for news outlets in South Africa, Jordan and Cambodia. He previously covered cybersecurity at ZDNet and TechRepublic.
