ROCCA GROUP PROFILES

APT Profile: CyberAv3ngers

AUGUST 3, 2026

Country of Origin	Iran
Threat Actor Type	State-sponsored
Other Names	Hydro Kitten, Storm-0784, APT Iran, Bauxite, Mr. Soul, Soldiers of Solor UNC5691, and Shahid Kaveh Group
Year Identified	2020
Target Countries	United States, Israel, United Kingdom, and Ireland

Profile Summary

CyberAv3ngers, also tracked as Hydro Kitten, Storm-0784, APT Iran, Bauxite, Mr. Soul, Soldiers of Solomon, UNC5691, and the Shahid Kaveh Group, is an active Iranian state-affiliated cyber threat actor linked to Iran's Islamic Revolutionary Guard Corps Cyber Electronic Command (IRGC-CEC) that conducts disruptive attacks against critical infrastructure and uses propaganda related to these attacks to align with Iranian state interests.

The group has been active since 2020, and was first observed conducting operational activities in 2023. CyberAv3ngers' operations reflect Iran's broader strategic use of cyber capabilities as a strategic tool to threaten adversary critical infrastructure globally and advance geopolitical objectives at a low cost and risk.

Their demonstrated ability to target and disrupt critical infrastructure through exploitation of vulnerable systems and the observed proliferation of their exploitation techniques to other cyber threat groups highlights the need for stronger cybersecurity standards, improved tracking of cyber threats, and coordinated policies to protect critical infrastructure from state-

directed cyber actors.

Most recently, in July 2026, CyberAv3ngers was linked to a coordinated cyber attack targeting more than 30 water systems in Minnesota, with related activity reported in several other states in the U.S.

Background and Development

CyberAv3ngers first emerged in 2020, and initially presented themselves as a hacktivist collective using the name "Cyber Avengers". The group claimed responsibility for a power outage and railway disruptions in Israel, but Israeli authorities found no evidence of cyber activity and attributed both incidents to technical faults. Although these claims were later discredited, they marked the beginning of CyberAv3ngers' public persona and demonstrated an early emphasis on information operations and psychological impact. In September 2023, the group resurfaced with the launch of their Telegram channel, @CyberAveng3rs, which it used to connect itself to the earlier 2020 claims, issue threats, publish target lists, and promote additional operations, some of which remained unverified.

CyberAv3ngers' operational capabilities and targeting have evolved in scope and technical complexity since their emergence. Their first verified attacks in late 2023 primarily exploited internet-exposed programmable logic controllers (PLC) that relied on default or weak passwords, enabling the group to compromise industrial control systems (ICS) with relatively simple techniques. Over time, the group began using increasingly sophisticated techniques. In 2024, researchers identified IOCONTROL, a custom malware platform designed to target Internet of Things (IoT) and operational technology (OT) devices, demonstrating a significant advancement in CyberAv3ngers' ability to conduct persistent operations against industrial environments. Around the same time, OpenAI disclosed that the group had used AI to assist with reconnaissance and debugging tasks, suggesting that CyberAv3ngers had begun integrating commercially available AI tools into their operational workflow. Recently, they shifted to exploiting CVE-2021-22681, a critical authentication bypass vulnerability affecting Rockwell Automation Logix controllers that cannot be remediated through a software patch alone. As their technical capabilities expanded, so too did their targeting. While early

campaigns focused primarily on Israeli-made devices and Israeli critical infrastructure, more recent operations have targeted globally deployed industrial systems, including widely used U.S.-manufactured equipment and U.S. critical infrastructure.

Most recently, in July 2026, CyberAv3ngers was linked to a coordinated cyber attack targeting more than 30 water systems in Minnesota, with related activity reported in several other states in the U.S. The operation reflected tactics that had been used in earlier campaigns, including targeting internet-exposed PLCs and OT environments in water and waterwaste facilities. However, the Minnesota campaign demonstrated a greater degree of operational coordination and scale than many of the group's previous operations. The attackers gained unauthorized access to ICS across multiple utilities, prompting local officials to request temporary reductions in water usage while systems were restored. Despite these operational impacts, officials reported no evidence that drinking water quality was compromised. This event reinforced CyberAv3ngers' sustained focus on critical infrastructure and suggested an increasing ability to conduct synchronized operations against multiple organizations simultaneously.

Several developments mark important turning points in CyberAv3ngers' evolution. The transition from making false or unverified claims between 2020 and 2023 to conducting verified cyber operations against critical infrastructure demonstrated a clear shift from propaganda to operational capability. Subsequent adoption of custom malware, AI-assisted operational support, and exploitation of advanced industrial control system vulnerabilities reflected continued growth in technical sophistication. These developments also prompted increased international attention. In early 2024, the U.S. Department of the Treasury sanctioned six officials associated with the IRGC-CEC for their connection to CyberAv3ngers. The U.S. Department of State's Rewards for Justice program currently offers up to $10 million for information leading to the identification or disruption of individuals associated with the group's cyber activities.

Organizational Structure

Although CyberAvengers initially portrayed themselves as a decentralized hacktivist collective, available evidence indicates that the group operates as a centralized, state-directed cyber

organization under Iran's IRGC-CEC. U.S. government agencies, including the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau Of Investigation (FBI), have attributed CyberAv3ngers to the IRGC-CEC. This assessment is further supported by actions taken by the U.S. Department of the Treasury, which sanctioned six IRGC-CEC officials for their roles in directing or supporting the group's cyber operations. These individuals include Hamid Reza Lashgarian, the head of the IRGC-CEC and an IRGC-Quds Force commander, along with Hamid Homayunfal, Mahdi Lashgarian, Milad Mansuri, Mohammad Amin Saberian, and Mohammad Bagher Shirinkar. Together, these attributions indicate that CyberAv3ngers functions as an operational arm of the IRGC rather than an independent hacktivist organization.

The group's internal organizational structure remains largely unknown. However, its operational history suggests a division of responsibilities typical of state-sponsored cyber organizations. CyberAv3ngers likely consists of technical operators responsible for network intrusions, malware developers who create and maintain specialized capabilities such as the IOCONTROL malware platform, intelligence personnel who identify and prioritize targets, and information or propaganda personnel who manage the group's public messaging through platforms such as Telegram. While the precise size and composition of these units cannot be confirmed, the coordination between technical operations and influence activities indicates an organized command structure capable of supporting sustained campaigns against critical infrastructure.

Similarly, little information exists regarding CyberAv3ngers' recruitment practices. Given their attribution to the IRGC-CEC, recruitment likely occurs through established IRGC channels, not through independent public recruitment efforts. Consistent with broader patterns observed among Iranian state-sponsored cyber organizations, members may be recruited from universities, technical institutes, and pro-Iranian hacktivist communities.

State and Non-State Relations & Strategic Objectives

CyberAv3ngers' primary objective is to advance Iranian political and strategic interests by demonstrating cyber capabilities, imposing costs on Israel and its supporters, and shaping

public perceptions. The group frequently targets Israeli and U.S. made technologies and critical infrastructure, combining disruptive attacks with Human-Machine Interface (HMI) defacements and propaganda statements, which signal to both the victims and the public that support for Israel can carry risk and cost. These operations often coincide with periods of heightened regional tensions, allowing Iran to project strength, reinforce anti-Israel narratives, and increase the psychological impact of its cyber activities.

Although CyberAv3ngers does not conduct cyber operations in direct support of battlefield activities, their campaigns advance broader, secondary military/security objectives. By targeting industrial control systems and other critical infrastructure, the group demonstrates an ability to disrupt essential services, pre-position access within critical networks, and collect information on vulnerable systems. These highly visible attacks also serve as deterrence signaling by showcasing Iran's capability to threaten critical infrastructure beyond its borders. However, there is no evidence that CyberAv3ngers conducts tactical cyber operations coordinated with conventional military forces, suggesting its role is one of strategic disruption rather than direct military support.

CyberAv3ngers has no identifiable economic objectives. Instead, its operations are driven by ideological and nationalist goals that closely align with Iranian regime interests. The group consistently portrays its attacks as retaliation against Israel and its allies while using HMI defacements to reinforce anti-Israel narratives and amplify the perceived impact of its operations. Despite its original presentation as a hacktivist collective, CyberAv3ngers' activities consistently support the broader strategic objectives of the Iranian government.

Target Profile

CyberAv3ngers primarily targets OT, ICS, and PLC that support critical infrastructure, particularly in the water and energy sectors. CyberAv3ngers' victim selection is driven by a combination of symbolic value, retaliation, and vulnerability. While the group frequently targets Israel directly, they also symbolically target Israel by attacking organizations that use Israeli-made technology, regardless of where the systems are deployed. These attacks frequently include HMI defacement, in many cases the statement "You have been hacked,

down with Israel. Every equipment ‘made in Israel’ is CyberAv3ngers legal target” is displayed on compromised systems following an attack. They also consistently target systems that are insecure due to internet exposure, weak or default passwords, or known vulnerabilities. This pattern demonstrates that CyberAv3ngers prioritizes targets that align with its ideological objectives while also offering a relatively low barrier to compromise.

Assessment of Impact

CyberAv3ngers poses a serious threat to national security because of their deliberate targeting of critical infrastructure that supports essential public services. Cyber operations have become an increasingly significant national security threat, allowing state-aligned actors to disrupt essential services, project influence, and achieve strategic objectives without the use of conventional military force. CyberAvengers’ operations have impacted water and water waste systems, energy infrastructure, and other operational technology environments and have the potential to further disrupt public services that are vital to public safety and government functions. Although the group has not primarily targeted military or intelligence networks, successful cyber attacks against critical infrastructure, especially during periods of geopolitical tension, could undermine public confidence, complicate emergency response, and strain government operations. As an Iranian state-aligned actor, CyberAv3ngers demonstrates how cyber capabilities can be leveraged to target vital infrastructure and services that civilians rely on, making the group a significant threat to national security.

While the group’s attacks have not been financially motivated, they still pose a moderate risk for economic impact. CyberAv3ngers has primarily caused indirect economic losses through service disruptions, operational downtime, and incident response and recovery costs. While attacks on critical infrastructure could produce localized economic consequences, the group has not demonstrated the capability or intent to inflict sustained or widespread economic damage.

CyberAv3ngers poses a high risk to public safety and political/social impacts due to their repeated targeting of operational technology supporting critical infrastructure, particularly within the water and energy sectors. Their attacks have the potential to disrupt services that

communities depend on while simultaneously amplifying fear and uncertainty through coordinated propaganda, defacement campaigns, and exaggerated public claims. As an IRGC-affiliated actor, CyberAv3ngers uses these operations to reinforce Iranian strategic messaging, increase psychological pressure on adversaries, and exploit periods of heightened geopolitical tension.

Beyond their immediate operational effects, CyberAv3ngers is likely to have a high long-term strategic impact by normalizing cyberattacks against civilian critical infrastructure and contributing to the spread of their tactics among other threat actors. By repeatedly targeting water, energy, and other essential services, the group has helped lower the threshold for future attacks on civilian infrastructure while eroding the international norms that have traditionally discouraged such operations. Their campaigns also increase the risk of escalation by creating opportunities for retaliation, miscalculation, or broader interstate conflict, particularly when cyber attacks coincide with military or political crises. Furthermore, CyberAv3ngers' ICS techniques have been adopted by over 60 affiliated cybercrime groups, extending the reach of its operational methods and increasing the likelihood that attacks against critical infrastructure will continue even if the group becomes inactive. All together, these factors suggest that CyberAv3ngers' long-term strategic impact stems not only from the attacks they've conducted, but also from their role in shaping a more permissive and enduring landscape for attacks on critical infrastructure.

Major Cyber Operations

Date	Operation / Target	Attack Type	Sector	Im
July 2026	Minnesota Water Systems	System Intrusion/ Hacking	Water and water waste systems	Wa acr coc

March 2026 – Present	Rockwell Automation Logix controllers	System Intrusion/ Hacking	Multiple Critical Infrastructure Sectors	Exp crit evo cau los
2024	Orpak and Gasboy fuel management systems	System Intrusion/ Hacking	Energy	Co and IOC abi dev evo ma sab
November 2023 – January 2024	Unitronics PLC defacement campaign	System Intrusion/ Hacking	Water and water waste systems	Co , in fac and hac in I
September – October 2023	Israeli OT and PLC devices	False Claim, System Intrusion/ Hacking, DoS/DDoS	Water, energy, shipping, distribution	Co cla infr 7 H
2020	Israeli power grid and railway	False claim	Energy, transportation	Fal att pro ope