INTRUVENT

THREAT ACTOR INTELLIGENCE PROFILE

CyberAv3ngers

IRGC Cyber-Electronic Command / BAUXITE / Soldiers of Solomon

Version 1.0
Last Updated March 17, 2026
Classification TLP:CLEAR
Attribution Confidence HIGH

Intruvent Technologies
INT-TAP-2026-CYBERAV3NGERS-v1.0

75+

Unitronics PLC/HMI Devices Compromised Since October 2023

First confirmed cyberattack on a US water utility | IRGC-CEC unit targeting OT/ICS systems globally

1 Attribution & Identity

ATTRIBUTION CONFIDENCE: HIGH

CyberAv3ngers is assessed with high confidence to be an offensive cyber operations unit within Iran's Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC). On February 2, 2024, the US Department of the Treasury's Office of Foreign Assets Control (OFAC) sanctioned six IRGC-CEC officials directly responsible for CyberAv3ngers operations against US critical infrastructure. The US Department of State's Rewards for Justice program has offered up to $10 million for information on these individuals. MITRE tracks this group as G1027.

Background

CyberAv3ngers is an Iranian state-sponsored group that targets industrial control systems (ICS) and operational technology (OT) environments, with a focus on water and wastewater utilities, fuel management systems, and dam infrastructure. Unlike most Iranian cyber operations groups that focus on IT environments, CyberAv3ngers directly attacks programmable logic controllers (PLCs), human-machine interfaces (HMIs), and embedded Linux devices in critical infrastructure.

The group gained international attention in November 2023 when it compromised the Municipal Water Authority of Aliquippa, Pennsylvania, marking the first confirmed cyberattack by an Iranian group against a US water utility. The attack exploited CVE-2023-6448, a default password vulnerability in Unitronics Vision Series PLCs, to deface HMI screens with anti-Israel messaging.

In December 2024, Claroty Team82 disclosed IOControl, a custom Linux malware framework deployed by CyberAv3ngers against IoT and OT devices including IP cameras, routers, PLCs, HMIs, and fuel management systems. IOControl uses MQTT for command and control, DNS-over-HTTPS for resolver queries, and modified UPX packing to evade detection. It represents a step change in the group's capability: from opportunistic defacement of internet-exposed PLCs to persistent backdoor access across diverse embedded device types.

Known Aliases

`CyberAv3ngers (Self-designated)` `BAUXITE (Dragos)` `Soldiers of Solomon` `IRGC-CEC Cyber Unit` `G1027 (MITRE)`

QUICK FACTS

- **Origin:** Iran (IRGC-CEC)
- **Active Since:** 2020 (earliest observed)
- **Motivation:** ICS/OT disruption, hacktivism
- **Sophistication:** Moderate to High
- **Last Observed:** Ongoing (IOControl deployment)
- **Sponsor:** IRGC Cyber-Electronic Command
- **Signature TTP:** Exploiting default PLC credentials
- **Custom Malware:** IOControl (Linux)
- **Sanctions:** OFAC (Feb 2024), 6 officials named
- **Bounty:** $10M Rewards for Justice

Sanctioned IRGC-CEC Officials

Source: US Treasury OFAC, February 2, 2024

Name	Role	Designation
Hamid Reza Lashgarian	Head of IRGC-CEC; commander of IRGC Quds Force Cyber Operations	OFAC SDN
Mahdi Lashgarian	IRGC-CEC official	OFAC SDN
Hamid Homayunfal	IRGC-CEC official	OFAC SDN
Milad Mansuri	IRGC-CEC official	OFAC SDN
Mohammad Bagher Shirinkar	IRGC-CEC official	OFAC SDN
Reza Mohammad Amin Saberian	IRGC-CEC official	OFAC SDN

> *"The deliberate targeting of critical infrastructure is an unconscionable threat to our national security. Today's actions hold accountable the Government of Iran and IRGC-affiliated individuals for their brazen attacks."*
>
> Under Secretary Brian E. Nelson, US Treasury Department, February 2, 2024

2 Targeting Profile

Industries

- **Water & Wastewater** (primary, 2023-present)
- **Fuel Management** (Gasboy/Orpak systems, 2023-2024)
- **Energy** (Israeli power infrastructure, 2020-2023)
- **Dams** (assessed targeting based on PLC exposure)
- **Manufacturing** (Unitronics PLC users)

Regions

- **Israel** (primary, 2020-present)
- **United States** (water utilities, 2023-present)
- **Ireland** (Eurotronics, Dec 2023)
- **Gulf States** (assessed)
- **Global** (any internet-exposed Unitronics PLC)

Technologies Targeted

- **Unitronics Vision PLCs** (TCP 20256)
- **Gasboy/Orpak Fuel Systems**
- **Hikvision IP Cameras**
- **D-Link Routers**
- **Dahua IP Cameras**
- **Linux-based IoT/OT Devices**

OT-First Targeting Approach

CyberAv3ngers bypasses traditional IT networks entirely. The group scans the internet for exposed OT devices, exploits default credentials or known vulnerabilities, and gains direct control of physical process equipment. This approach circumvents IT-centric defenses (EDR, SIEM, firewalls) because the targeted devices often lack security monitoring altogether.

3 Tactics, Techniques & Procedures

MITRE ATT&CK for ICS

INITIAL ACCESS (ICS)

- `T0812` ICS Default Credentials
- `T0883` ICS Internet Accessible Device

EXECUTION (ICS)

- `T0814` ICS Denial of Service

IMPACT (ICS)

- `T0826` ICS Loss of Availability
- `T0828` ICS Loss of Productivity and Revenue
- `T0829` ICS Loss of View

MITRE ATT&CK Enterprise

INITIAL ACCESS

- `T1078.001` Default Accounts
- `T1110` Brute Force

EXECUTION

- `T1059` Command and Scripting Interpreter

PERSISTENCE

- `T1547` Boot or Logon Autostart Execution

DEFENSE EVASION

- `T1027.002` NOVEL Software Packing (modified UPX)

DISCOVERY

- `T1082` System Information Discovery
- `T1046` Network Service Discovery

COMMAND AND CONTROL

- `T1071.001` NOVEL Application Layer Protocol (MQTT)

IMPACT

- `T1499` Endpoint Denial of Service
- `T1491.001` Internal Defacement
- `T1565.001` Stored Data Manipulation
- `T1531` Account Access Removal

Novel Techniques

MQTT-Based C2 from OT Devices

IOControl uses MQTT (Message Queuing Telemetry Transport) over port 8883 (TLS) for command and control. MQTT is a lightweight IoT protocol rarely monitored by security tools. The malware publishes status reports and receives commands through an MQTT broker, blending C2 traffic with legitimate IoT telemetry. This is the first documented use of MQTT as a primary C2 channel by an Iranian state-sponsored actor. (Source: Claroty Team82, December 2024)

DNS-over-HTTPS from OT Networks

IOControl resolves C2 domain names using DNS-over-HTTPS (DoH) via Cloudflare's 1.1.1.1 resolver. OT devices and embedded Linux systems do not generate DoH traffic under normal operating conditions. Any DoH request originating from an OT network segment is a high-fidelity anomaly indicator. (Source: Claroty Team82, December 2024)

Modified UPX Packing

IOControl binaries are packed with a modified version of UPX that replaces the standard magic bytes ("UPX!") with "ABC!" to prevent standard UPX unpacking tools from decompressing the binary. This simple but effective technique breaks automated analysis pipelines that rely on recognizing standard UPX headers. (Source: Claroty Team82, December 2024)

4 Tooling & Infrastructure

IOControl Malware

IOControl is CyberAv3ngers' custom Linux malware framework, first disclosed by Claroty Team82 in December 2024. It is designed for deployment on IoT and OT devices running embedded Linux, including IP cameras (Hikvision, Dahua), routers (D-Link), PLCs (Unitronics), and fuel management systems (Gasboy/Orpak).

Attribute	Detail
Type	Linux backdoor / remote access trojan
Target Platforms	Embedded Linux (ARM, MIPS, x86)
C2 Protocol	MQTT over TLS (port 8883)
DNS Resolution	DNS-over-HTTPS via Cloudflare (1.1.1.1)
Packing	Modified UPX with "ABC!" magic bytes (replaces standard "UPX!")
Installation Path	`/usr/bin/iocontrol`
Persistence	Init script at `/etc/rc3.d/S93InitSystemd.sh`
Temp Directory	`/tmp/iocontrol/`
Capabilities	Command execution, self-delete, port scanning, persistence, system reconnaissance
Source	Claroty Team82 (December 2024)

IOControl Infection Chain

Source: Claroty Team82, December 2024

STEP 1: INITIAL ACCESS

- Scan internet for exposed OT/IoT devices (Shodan, custom scanners)
- Exploit default credentials (CVE-2023-6448) or known vulnerabilities
- Gain shell access to embedded Linux operating system

↓

STEP 2: MALWARE DEPLOYMENT

- Download IOControl binary (modified UPX packed, "ABC!" magic bytes)
- Install to `/usr/bin/iocontrol`
- Create persistence script at `/etc/rc3.d/S93InitSystemd.sh`

↓

STEP 3: C2 ESTABLISHMENT

- Resolve C2 domain via DNS-over-HTTPS (Cloudflare 1.1.1.1)
- Connect to MQTT broker on port 8883 (TLS)
- Register device with unique identifier; await commands

↓

STEP 4: OPERATIONAL CONTROL

- Execute arbitrary commands on compromised device
- Conduct network reconnaissance and port scanning
- Manipulate device functions (PLC logic, HMI display, fuel system data)
- Self-delete capability to destroy forensic evidence

C2 Infrastructure

Indicator	Type	Context	Source
`159.100.6.69`	IP Address	IOControl C2 server	Claroty Team82 (Dec 2024)
`uuokhhfsdlk.tylarion867mino.com`	Domain	IOControl C2 domain	Claroty Team82 (Dec 2024)
`ocferda.com`	Domain	IOControl C2 domain	Claroty Team82 (Dec 2024)

C2 domains are resolved via DNS-over-HTTPS to avoid standard DNS monitoring. MQTT connections use TLS on port 8883. Infrastructure attribution to CyberAv3ngers is based on Claroty Team82 analysis linking IOControl deployment to previously attributed CyberAv3ngers operations.

5 Notable Campaigns

Aliquippa PA Water Authority Compromise

November 25, 2023

Water/Wastewater · United States · Unitronics Vision

First confirmed cyberattack by an Iranian state actor against a US water utility. CyberAv3ngers exploited CVE-2023-6448 (default password "1111") on an internet-exposed Unitronics Vision PLC at the Municipal Water Authority of Aliquippa, Pennsylvania. The attackers defaced the HMI screen with the message: "You have been hacked. Down with Israel. Every equipment 'made in Israel' is CyberAv3ngers legal target." The compromised device controlled a booster station regulating water pressure. Operators switched to manual control, and no disruption to water service occurred. CISA issued Advisory AA23-335A on December 1, 2023.

Unitronics PLC Defacement Wave

October 2023 - January 2024

Water/Wastewater · Energy · Global · Unitronics Vision

Broader campaign targeting internet-exposed Unitronics Vision PLCs worldwide. CISA confirmed at least 34 US water and wastewater facilities were targeted. Open-source reporting indicates 75+ devices were accessed globally. All attacks exploited CVE-2023-6448 (default credentials) and TCP port 20256. The campaign followed a consistent pattern: scan for exposed devices, authenticate with default password "1111," replace HMI display with anti-Israel propaganda, and in some cases modify PLC operational parameters. (Sources: CISA AA23-335A; CISA update December 2024)

Israeli Water Stations

October 2023

Water/Wastewater · Israel · Unitronics Vision

CyberAv3ngers claimed to have compromised 10 water treatment stations in Israel. The attacks occurred in the immediate aftermath of the October 7, 2023 Hamas attack and appear to have been an IRGC-directed response through the cyber domain. Attacks targeted Unitronics PLCs controlling water treatment processes. Israel's National Cyber Directorate issued warnings to water sector operators. (Sources: Dragos; CSIS "Beyond Hacktivism," January 2026)

Orpak/Gasboy Fuel Management Systems

October 2023 - August 2024

Fuel Management · Israel · United States · Gasboy/Orpak

Two-wave campaign targeting fuel management systems. The first wave (October 2023) targeted Israeli gas stations using Orpak systems, with CyberAv3ngers claiming approximately 200 gas stations affected. The second wave expanded to Gasboy fuel management systems in the United States. IOControl malware was deployed on compromised fuel management devices, providing persistent backdoor access. Claroty Team82 confirmed IOControl samples were recovered from Gasboy fuel management systems in the US. (Sources: Claroty Team82, December 2024; Dragos)

IP Camera and Router IOControl Deployment

2024 - Ongoing

IoT/OT · Global · Hikvision · D-Link · Dahua

Ongoing campaign deploying IOControl malware on compromised IP cameras (Hikvision, Dahua) and routers (D-Link). These devices serve as entry points into OT networks and as relay infrastructure. The campaign expands CyberAv3ngers' foothold beyond PLCs and fuel systems into the broader IoT ecosystem surrounding critical infrastructure. (Source: Claroty Team82, December 2024)

6 Detection & Response

Detection Opportunities

Network-Based Detection

- > MQTT traffic (port 8883 TLS) originating from OT network segments
- > DNS-over-HTTPS requests to 1.1.1.1 from devices that should not make DoH queries
- > Connections to known C2 IPs and domains (see Appendix A)
- > Outbound traffic from PLCs, HMIs, or embedded devices to internet destinations
- > TCP 20256 connections to Unitronics PLCs from external IPs

Host-Based Detection

- > File `/usr/bin/iocontrol` on Linux-based IoT/OT devices
- > Persistence script `/etc/rc3.d/S93InitSystemd.sh`
- > Directory `/tmp/iocontrol/`
- > Binaries with modified UPX headers ("ABC!" instead of "UPX!")
- > SHA256 hash match for IOControl binary

PLC/HMI Monitoring

- > Unauthorized changes to HMI display content (defacement)
- > Modifications to PLC ladder logic or program memory
- > Login events using default credentials on Unitronics devices
- > Configuration changes to PLC communication parameters

Fuel Management Systems

- > Anomalous processes on Gasboy/Orpak terminals
- > Unexpected outbound connections from fuel management networks
- > File system changes on fuel management controllers
- > Discrepancies between physical fuel levels and reported data

Defensive Recommendations

Priority 1: Remove ICS/OT Devices from the Internet

CyberAv3ngers' entire attack surface depends on internet-exposed OT devices. Disconnecting PLCs, HMIs, fuel management systems, and IP cameras from direct internet access eliminates the primary attack vector. If remote access is required, place devices behind a VPN with multi-factor authentication.

Priority 2: Change All Default Credentials

CVE-2023-6448 exists because Unitronics Vision PLCs ship with a default password of "1111." Audit all PLC, HMI, IP camera, and router credentials. Change every default password. Implement unique, complex passwords for each device. This single action would have prevented every Unitronics compromise in the 2023-2024 campaign.

Priority 3: Implement OT Network Segmentation

OT devices should reside on isolated network segments with strict firewall rules controlling traffic between OT and IT networks. Block MQTT (port 8883), DNS-over-HTTPS, and all unnecessary outbound connections from OT segments. Monitor for any traffic crossing segmentation boundaries.

Priority 4: Monitor for IOControl Indicators

Deploy file integrity monitoring on Linux-based IoT/OT devices where feasible. Search for IOControl artifacts: `/usr/bin/iocontrol`, `/etc/rc3.d/S93InitSystemd.sh`, `/tmp/iocontrol/`. Monitor for MQTT traffic on port 8883 and DoH traffic to 1.1.1.1 from OT network segments.

Priority 5: Implement PLC Program Integrity Monitoring

Maintain known-good backups of PLC ladder logic and HMI configurations. Periodically compare running programs against baselines to detect unauthorized modifications. Unitronics VisiLogic software supports program upload and comparison.

A Appendix A: Indicators of Compromise

File Indicators

Type	Value	Context	Source
SHA256	`1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498`	IOControl malware binary	Claroty Team82 (Dec 2024)
File Path	`/usr/bin/iocontrol`	IOControl installation path	Claroty Team82 (Dec 2024)
File Path	`/etc/rc3.d/S93InitSystemd.sh`	IOControl persistence script	Claroty Team82 (Dec 2024)
Directory	`/tmp/iocontrol/`	IOControl temporary working directory	Claroty Team82 (Dec 2024)
UPX Magic	`ABC!` (replaces standard `UPX!`)	Modified UPX packing signature	Claroty Team82 (Dec 2024)

Network Indicators

Type	Value	Context	Source
IP Address	`159.100.6.69`	IOControl C2 server	Claroty Team82 (Dec 2024)
Domain	`uuokhhfsdlk.tylarion867mino.com`	IOControl C2 domain	Claroty Team82 (Dec 2024)
Domain	`ocferda.com`	IOControl C2 domain	Claroty Team82 (Dec 2024)
Port	TCP 8883	MQTT over TLS (C2 channel)	Claroty Team82 (Dec 2024)
Port	TCP 20256	Unitronics PCOM protocol (target access)	CISA AA23-335A

IOC Blocking Guidance

Tier 1: Block (High Confidence)

SHA256 hash, file paths, C2 domains (uuokhhfsdlk.tylarion867mino.com, ocferda.com): These are confirmed CyberAv3ngers infrastructure with no legitimate use case. Safe to add to firewall deny rules, DNS sinkholes, and endpoint detection blocklists.

Tier 2: Alert/Monitor (Shared Infrastructure)

IP 159.100.6.69: This IP is associated with IOControl C2 infrastructure based on Claroty Team82 analysis. Verify current hosting provider and whether the IP is part of shared infrastructure before implementing a network-level block. Deploy as a detection/alerting indicator; require analyst review before action. **Port 8883 (MQTT):** MQTT is a legitimate IoT protocol. Do not block port 8883 globally. Alert on MQTT traffic originating from OT network segments where it is unexpected.

Tier 3: Investigate (Contextual)

Port 20256 (Unitronics PCOM): This is a legitimate Unitronics protocol port. Blocking it will disrupt PLC communications. Instead, restrict access to this port to authorized management stations only. Investigate any external (internet-sourced) connections to this port. **DNS-over-HTTPS to 1.1.1.1:** Cloudflare's resolver is used by millions of legitimate users. Do not block 1.1.1.1. Instead, alert on DoH traffic from OT network segments where it should not occur.

B Appendix B: References

Sources

[1] CISA, "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities," Advisory AA23-335A, December 1, 2023 (updated December 2024). https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-335a

[2] Claroty Team82, "IOControl: New Malware Used by CyberAv3ngers to Target Critical Infrastructure," December 2024. https://claroty.com/team82/research/iocontrol-cyberav3ngers-malware

[3] US Department of the Treasury, "Treasury Sanctions IRGC-Affiliated Cyber Actors for Roles in Targeting Critical Infrastructure," February 2, 2024. https://home.treasury.gov/news/press-releases/jy2072

[4] MITRE ATT&CK, "CyberAv3ngers - G1027." https://attack.mitre.org/groups/G1027/

[5] Trellix, "The Iranian Cyber Capability 2026," March 5, 2026.

[6] CSIS, "Beyond Hacktivism: How Iran's Proxy Hackers Became a National Security Problem," January 14, 2026.

[7] Dragos, "BAUXITE Threat Group Assessment," 2024.

[8] Intruvent Technologies, Golden CTI Database. CVE-2023-6448 record: CISA KEV, actively exploited, Unitronics Vision PLC and HMI. Sector targeting data: Water/Wastewater (MEDIUM confidence), Dams (MEDIUM confidence).

[9] CISA, "Unitronics PLC Default Password Vulnerability," CVE-2023-6448, CISA Known Exploited Vulnerabilities Catalog, added December 11, 2023.

TRACK THIS THREAT ACTOR CONTINUOUSLY

BRACE monitors CyberAv3ngers and 275+ threat actors with sector-specific intelligence, detection rules, and automated alerting.

- ✓ Real-time threat actor tracking
- ✓ Sector-specific risk scoring (ITR)
- ✓ Detection rules updated with each reporting cycle

See BRACE Plans →

or

Need incident response or forensics support? Contact us at contact@intruvent.com