

Threat Intelligence Report: IRGC-Affiliated OT/IoT Malware Evolution



krypt3ia.wordpress.com/2026/04/30/threat-intelligence-report-irgc-affiliated-ot-iot-malware-evolution

April 30, 2026



[leave a comment »](#)

Executive Assessment

Iran-linked operational technology (OT) cyber activity has progressed from opportunistic access and symbolic defacement into a more structured, implant-enabled capability set. The inflection point is IOCONTROL, a custom Linux/ARM OT-IoT backdoor attributed to CyberAv3ngers, a persona assessed as affiliated with the IRGC Cyber-Electronic Command. IOCONTROL introduces durable persistence, encrypted configuration (AES-class schemes), MQTT-based command-and-control, device profiling, arbitrary command execution, internal scanning, and self-delete functionality across embedded OT/IoT systems. As documented by Claroty, it has been

observed in real environments, including Orpak/Gasboy fuel-management deployments, establishing it as an operational access tool against civilian critical infrastructure rather than a purely demonstrative artifact.

CyberAv3ngers (IOCONTROL) — Threat Level: High.

CyberAv3ngers has moved beyond exposed-PLC defacement into repeatable, malware-backed access across OT-adjacent Linux devices (fuel controllers, gateways, routers, and similar appliances). IOCONTROL's MQTT C2 model, persistence via init scripts, and cross-vendor targeting enable scalable footholds and coordinated tasking. While it does not yet evidence deterministic PLC logic manipulation, the combination of persistent access, lateral reconnaissance, and command execution materially increases disruption risk in fuel distribution and other services where OT/IoT intermediaries are critical. The actor's prior focus on Israeli-linked infrastructure and demonstrated deployment elevates both intent and credibility.

ZionSiphon — Threat Level: Low to Moderate.

ZionSiphon is best assessed as an OT-themed, immature artifact. Analyses from Darktrace highlight water-sector targeting strings (e.g., chlorine dosing and RO pressure), but subsequent scrutiny referenced from Dragos indicates broken execution paths, absence of a functional ICS communication stack, and no credible C2. The code remains confined to the Windows host layer and lacks viable pathways to PLC interaction. It signals intent and contributes to psychological effect, but in its current form is not a reliable cyber-physical weapon.

IRGC enterprise intrusion clusters (e.g., APT33 / Peach Sandstorm and related groups) — Threat Level: High.

These actors maintain mature IT-centric tradecraft—phishing, credential theft, webshelling, and custom backdoors (e.g., multi-stage implants like Tickler)—to achieve persistent access in defense, energy, and telecom sectors. Their strength is depth and stealth in enterprise environments rather than OT-native manipulation. They present high strategic risk through pre-positioning and intelligence collection that can enable follow-on disruption.

Destructive operators (e.g., Agrius) — Threat Level: High.

Agrius and similar clusters employ wipers (often masked as ransomware) to achieve punitive or coercive effects, particularly against Israeli targets. Their capability is well demonstrated in enterprise networks; when such activity intersects with OT-connected environments, it can cascade into operational outages. The risk profile is high due to willingness to deploy destructive payloads.

Synthesis.

The ecosystem now separates into three lanes: enterprise espionage, destructive enterprise operations, and OT/IoT coercion. CyberAv3ngers is the clearest representative of the third lane, with IOCONTROL as its operational benchmark. ZionSiphon sits at the experimental edge of that lane—indicative of direction but not capability. Overall, Iran's OT posture remains uneven but is

advancing: IOCONTROL closes the gap between IT-style implants and OT-adjacent systems, while parallel IRGC units sustain high-end access and destructive options that can be combined for broader impact.

Actor Attribution

Primary actor: CyberAv3ngers / Cyber Av3ngers / CyberAveng3rs
Assessed sponsor alignment: IRGC Cyber-Electronic Command
Associated malware family: IOCONTROL / [elf.iocontrol](#)
Operational focus: Israeli-linked OT/IoT systems, U.S. critical infrastructure, fuel systems, water systems, PLC/HMI devices, and internet-exposed embedded platforms.

Claroty states that IOCONTROL was extracted from a Gasboy fuel-management system allegedly compromised by CyberAv3ngers, and that the group is believed to be part of the IRGC Cyber-Electronic Command. ([Claroty](#)) Malpedia also associates CyberAv3ngers with [elf.iocontrol](#) and records the actor’s historical claims against Israeli critical infrastructure. ([malpedia.caad.fkie.fraunhofer.de](#))

Malware Comparison

Capability	Earlier CyberAv3ngers Activity	IOCONTROL	ZionSiphon
Primary target	Unitronics PLC/HMI devices, water utilities	OT/IoT Linux devices, fuel systems, PLCs, HMIs, routers, firewalls	Israeli water/desalination-themed environments
Main effect	Defacement, access demonstration, fear generation	Persistent access, command execution, scanning, potential disruption	Intended sabotage, but likely nonfunctional
C2	Not strongly evidenced publicly	MQTT-based C2 over IoT-style channels	No credible mature C2 model identified
Persistence	Device/configuration abuse	Boot persistence via Linux init path	Windows host persistence mechanisms
Technical maturity	Low to moderate	Moderate to high for OT/IoT malware	Low
Operational credibility	Confirmed access to exposed OT	Confirmed implant sample and victim-specific configuration	Disputed; likely prototype or influence artifact

IOCONTROL Technical Profile

IOCONTROL is a Linux-based backdoor designed for embedded OT/IoT platforms. Claroty reports that it has been used against routers, PLCs, HMIs, firewalls, IP cameras, and fuel-management systems from vendors including Orpak, Gasboy, Unitronics, Phoenix Contact, Teltonika, Hikvision, D-Link, Red Lion, and others. ([Claroty](#))

The analyzed sample:

[1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498](#)

Claroty reports the sample was compiled for **ARM 32-bit big-endian Linux**, used a modified UPX-like packing method, and decrypted configuration entries using **AES-256-CBC**. It used MQTT for C2 and was configured with victim-specific identifiers. ([Claroty](#))

Core functions include:

- Host and device profiling.
- MQTT-based beaconing and command tasking.
- Arbitrary OS command execution.
- Output exfiltration.
- Internal scanning.
- Self-delete.
- Boot persistence.

This makes IOCONTROL more than an OT scareware artifact. It is not Stuxnet-class process manipulation, but it is a real embedded-device implant with operational utility.

ZionSiphon Technical Profile

ZionSiphon appears to be an OT-themed malware sample built around Israeli water-sector targeting. Darktrace identifies water-treatment and desalination strings, including references to Israeli desalination sites and water-sector components. ([Darktrace](#))

However, its operational value is doubtful. Dragos' public assessment, as reported by CyberScoop, states that the code is broken, shows little to no knowledge of ICS protocols, contains likely LLM-generated fictional paths and process names, and would not pose a meaningful threat to real water plants even if its targeting logic were corrected. ([CyberScoop](#))

Analytic judgment: *ZionSiphon is best treated as a prototype, influence artifact, or low-quality experiment—not a validated deployable ICS weapon.*

Strategic Interpretation

CyberAv3ngers' evolution shows a clear trajectory:

Stage 1: Symbolic OT access

The actor abused exposed PLC/HMI systems to display political messages, causing alarm disproportionate to the technical sophistication.

Stage 2: OT-adjacent disruption

The actor expanded into fuel-management systems, where compromise of Linux payment terminals and site controllers could interrupt service availability and create public-sector concern.

Stage 3: Implant-enabled OT/IoT access

IOCONTROL gives the actor persistence, command execution, scanning, and centralized tasking across embedded systems.

Stage 4: Influence-amplified malware narratives

ZionSiphon-like artifacts suggest Iranian-aligned or anti-Israel actors may increasingly use ICS-themed malware narratives to generate psychological effect even where the code is immature.

Threat to Critical Infrastructure

The highest-risk environments are not necessarily deeply engineered PLC networks. They are **OT-adjacent Linux appliances** sitting between enterprise IT and physical processes:

- Fuel payment terminals.
- Site controllers.
- PLC/HMI gateways.
- Routers and cellular gateways.
- Firewalls.
- Cameras.
- Remote access appliances.
- Industrial IoT monitoring devices.

These systems are often internet-exposed, poorly inventoried, weakly segmented, and inconsistently patched. IOCONTROL directly exploits this defensive blind spot.

Detection and Hunting Priorities

Priority artifacts:

/usr/bin/iocontrol

/tmp/iocontrol

/var/run/iocontrol.pid

/etc/rc3.d/S93InitSystemd.sh

Network indicators to hunt:

uuokhhfsdlk.tylarion867mino[.]com

159[.]100[.]6[.]69

ocferda[.]com

104[.]21[.]62[.]225

172[.]67[.]139[.]215

3[.]217[.]232[.]142

Behavioral detections:

- MQTT traffic from OT/IoT devices to unknown external brokers.
- TCP/8883 or TCP/1883 from embedded devices that do not normally use MQTT.
- New init scripts under `/etc/rc*.d/`.
- Unknown ELF binaries on ARM/MIPS/Linux appliances.
- Outbound DNS-over-HTTPS from OT-adjacent devices.
- Internal port scanning sourced from fuel systems, HMIs, cameras, routers, or PLC gateways.
- Repeated device inventory collection from embedded Linux hosts.

Analytic Confidence

High confidence: IOCONTROL is tied to CyberAv3ngers and Iran-affiliated OT/IoT activity.

High confidence: IOCONTROL represents a technical upgrade from CyberAv3ngers' earlier exposed-PLC defacement activity.

Moderate confidence: IOCONTROL reflects an IRGC-aligned effort to develop scalable OT/IoT coercive capability.

Low to moderate confidence: ZionSiphon is connected to the same actor set. It is better assessed as part of the broader Iran/Israel OT influence environment than as confirmed CyberAv3ngers tooling.

Low confidence: ZionSiphon has meaningful real-world destructive capability.

Conclusion

IOCONTROL is the operational benchmark for Iranian-linked OT/IoT malware. ZionSiphon is the warning signal. Together, they show that Iranian-aligned actors are experimenting aggressively in the OT domain, but capability remains uneven: CyberAv3ngers has demonstrated credible embedded-device access, while ZionSiphon currently looks more like an immature psychological or prototype artifact than a functioning cyber-physical weapon.

Appendix A — Consolidated Indicators of Compromise (IOCs)

Scope: IOCONTROL (CyberAv3ngers), ZionSiphon (low-confidence / prototype), and related IRGC-affiliated activity where directly relevant.

Note: IOC fidelity varies. IOCONTROL indicators are **high confidence**. ZionSiphon indicators are **low confidence / contextual** due to questionable operational validity.

1. IOCONTROL (CyberAv3ngers) — High Confidence

File Hashes

SHA256: 1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498

SHA256: bc160db9bdf6758cafaa1940b8cbe1608fe3f236743d312a08568fa0fb1250ab

SHA1: 366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb

MD5: c92e2655d115368f92e7b7de5803b7bc

Domains

uuokhhfsdlk.tylarion867mino[.]com

ocferda[.]com

IP Addresses

159[.]100[.]6[.]69 (Primary MQTT C2)

104[.]21[.]62[.]225 (Cloudflare fronting)

172[.]67[.]139[.]215 (Cloudflare fronting)

3[.]217[.]232[.]142 (AWS infrastructure)

Network / Protocol Indicators

TCP/8883 (MQTT over TLS)

TCP/1883 (MQTT)

TCP/15672 (RabbitMQ management panel)

MQTT Behavioral Patterns

{GUID}/hello

{GUID}/push

{GUID}/output

File System Artifacts

/usr/bin/iocontrol

/tmp/iocontrol

/var/run/iocontrol.pid

/etc/rc3.d/S93InitSystemd.sh

Persistence Mechanism

Linux init script execution via rc3.d

Behavioral Indicators

- MQTT beaconing from OT/IoT devices
- Encrypted config (AES-256-CBC)
- DNS-over-HTTPS usage
- Internal network scanning from embedded devices
- Arbitrary command execution via broker tasking
- Self-delete capability

2. CyberAv3ngers (Pre-IOCONTROL Activity) — Moderate Confidence

Known Tradecraft Indicators (Non-Malware)

Default credentials on Unitronics PLCs

Internet-exposed HMI panels

Shodan/Censys discovery patterns

Victim-Facing Indicators

Unauthorized HMI message displays

PLC logic interruption / loss of view

Network Indicators (Behavioral)

- Direct web access to PLC management interfaces
- Unauthenticated or weakly authenticated remote access attempts

3. ZionSiphon — Low Confidence / Prototype Artifact

File / Behavioral Indicators

Sha256[07c3bbe60d47240df7152f72beb98ea373d9600946860bad12f7bc617a5d6f5f](#)

Embedded Strings / Targeting Artifacts

Mekorot

SCADA_SecurityPatch_v8.4.exe

Chlorine_Dose=10

Chlorine_Flow=MAX

Chlorine_Pump=ON

Chlorine_Valve=OPEN

RO_Pressure=80

Network Indicators

(No confirmed C2 infrastructure)

(No validated beaconing pattern)

Behavioral Indicators

- Windows host execution (not PLC-native)
- Registry-based persistence
- PowerShell execution chains
- USB propagation attempts
- ICS protocol references (Modbus, DNP3, S7) — **non-functional / incomplete**
- No confirmed PLC communication stack

4. IRGC-Linked Enterprise Intrusion (Contextual Only)

(Included for correlation; not directly IOCONTROL-linked)

Common Indicators

Webshell deployment (IIS / Exchange)

LSASS dumping artifacts

Credential harvesting tools

Infrastructure Patterns

- VPS-hosted C2
- Cloud-based staging (AWS, VPS providers)
- Use of compromised infrastructure

Detection Prioritization

Tier 1 (Immediate Action)

- IOCONTROL hashes
- Known IOCONTROL domains/IPs
- MQTT traffic from OT/IoT devices

Tier 2 (High Signal Behavioral)

- Unknown ELF binaries on embedded systems
- New init scripts in `/etc/rc*.d/`
- Outbound DoH from OT devices
- Internal scanning from OT network segments

Tier 3 (Contextual / Investigative)

- ZionSiphon strings in logs or binaries
- ICS-themed malware without C2
- Suspicious OT-focused PowerShell execution

Rate this:

Rate This

Written by Krypt3ia

2026/04/30 at 14:28

Posted in [Uncategorized](#)

Tagged with [ai](#), [cyber-security](#), [Cybersecurity](#), [Security](#), [technology](#)

« [Threat Analysis Report: AI Enhanced Infrastructure Attacks At Scale on Critical Infrastructure](#)

[Islamic Cyber Resistance in Iraq 313 \(ICR-313\) Ubuntu DDOS Actor Profile](#) »

Leave a comment

This site uses Akismet to reduce spam. [Learn how your comment data is processed.](#)