INTRUVENT

THREAT ACTOR INTELLIGENCE PROFILE

Hydro Kitten

IRGC-CEC Shahid Kaveh / CyberAv3ngers / BAUXITE / G1027

Version 1.0
Last Updated March 18, 2026
Classification TLP:CLEAR
Attribution Confidence HIGH

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

6

IRGC-CEC Officials Sanctioned by U.S. Treasury

ICS/IoT destruction group now threatening Western financial sector (CrowdStrike, March 2026)

1 Attribution & Identity

ATTRIBUTION CONFIDENCE: HIGH

Hydro Kitten is assessed with high confidence to operate on behalf of Iran's Islamic Revolutionary Guard Corps Cyber-Electronic Command (IRGC-CEC), specifically the Shahid Kaveh sub-unit. CrowdStrike tracks this actor under the "Hydro Kitten" designation and describes it as a "likely Iran-nexus targeted intrusion adversary." MITRE ATT&CK tracks the overlapping CyberAv3ngers cluster as G1027. CISA, FBI, NSA, and Israeli INCD jointly attributed CyberAv3ngers activity to the IRGC in Advisory AA23-335A (December 2023). Six IRGC-CEC officials were sanctioned by the U.S. Department of the Treasury in February 2024 for their roles in CyberAv3ngers operations.

Background

Hydro Kitten is CrowdStrike's designation for a threat activity cluster attributed to the IRGC-CEC Shahid Kaveh sub-unit. This sub-unit is reportedly responsible for researching critical infrastructure vulnerabilities and conducting cyber-related propaganda operations. The group has been active since at least 2020, initially focusing on Israeli critical infrastructure before expanding to global targets.

The actor operates through several public-facing personas, including CyberAv3ngers, Soldiers of Solomon, and various "Mr. Soll" / "Mr. Soul" accounts. These personas conduct defacement campaigns, DDoS operations, and destructive attacks against industrial control systems (ICS) and Internet of Things (IoT) devices. The group's stated objectives are destruction, defacement, and denial of service.

In early 2026, CrowdStrike published a financial sector targeting advisory identifying Hydro Kitten as an explicit threat to Western financial institutions. This represents a significant expansion from the group's documented ICS/OT focus into the financial services sector, coinciding with the escalation of the U.S.-Israel-Iran conflict (Operation Epic Fury, February 2026).

Known Aliases

`Hydro Kitten (CrowdStrike)` `CyberAv3ngers` `BAUXITE (Dragos)` `G1027 (MITRE)` `Soldiers of Solomon`

Operational Personas

These are cover identities used for specific campaigns, not separate threat actors.

`CyberAv3ngers` `Soldiers of Solomon` `Mr. Soll / mrsoul_group` `Mr_S0ull / mr_soul0` `Mr Soul / Mr.Soul`

QUICK FACTS

- **Origin:** Iran (IRGC-CEC)
- **Sub-unit:** Shahid Kaveh
- **Active Since:** 2020 (earliest observed)
- **Motivation:** State-sponsored ICS/OT disruption; financial sector targeting
- **Sophistication:** Moderate to High
- **Last Observed:** March 2026 (financial sector threats)
- **Signature TTP:** Unitronics PLC exploitation via default credentials
- **Custom Malware:** IOCONTROL
- **Sanctions:** 6 officials (U.S. Treasury, Feb 2024)

> *"Much of the activity being publicized appears to be claim-driven rather than evidence-backed."*
>
> Adam Meyers, Head of Counter Adversary Operations, CrowdStrike (March 2026), on Hydro Kitten's public claims

Source Limitation Notice

Hydro Kitten has limited public documentation compared to longer-established Iranian APT groups. CrowdStrike's adversary profile and the joint CISA/FBI/NSA advisory on CyberAv3ngers (AA23-335A) are the primary authoritative sources. The March 2026 financial sector targeting advisory from CrowdStrike has not been independently corroborated by other vendors at time of publication. Sections of this profile that rely on single-source reporting are marked accordingly.

2 Targeting Profile

Industries

- **Water / Wastewater** (primary, 2023-present)
- **Energy / Fuel Management** (2024-present)
- **Food & Beverage** (2023)
- **Healthcare** (2023)
- **Financial Services** (new, 2026; per CrowdStrike)
- **Critical Infrastructure** (broad, ongoing)

Regions

- **Israel** (primary, 2020-present)
- **United States** (water utilities, 2023-present)
- **Ireland** (water utility, 2023)
- **Western nations** (financial sector, 2026)
- **Allied nations** (per CISA AA23-335A)

Technologies Targeted

- **Unitronics Vision Series PLCs** (default TCP 20256)
- **Linux-based IoT devices** (IOCONTROL)
- **Baicells, D-Link, Hikvision routers/cameras**
- **Orpak fuel management systems**
- **Teltonika cellular gateways**
- **Internet-exposed SCADA/HMI**

Financial Sector Expansion (March 2026)

CrowdStrike's financial sector targeting advisory identified Hydro Kitten as explicitly threatening Western financial institutions. This coincided with the group's DDoS threats against U.S. banking infrastructure. The financial sector expansion reportedly aligns with broader IRGC objectives during the escalating U.S.-Israel-Iran military conflict. CrowdStrike's Adam Meyers noted that much of the publicized activity appears "claim-driven rather than evidence-backed," suggesting the DDoS threats may be more aspirational than operational. [REQUIRES VERIFICATION: Independent corroboration of financial sector intrusion activity has not been published by other vendors at time of writing.]

3 Tactics, Techniques & Procedures

The following techniques are documented for the CyberAv3ngers cluster (MITRE G1027) and related Hydro Kitten activity, sourced from MITRE ATT&CK, CISA AA23-335A, and Claroty Team82 research.

INITIAL ACCESS

`T1190`	Exploit Public-Facing Application
`T1078.001`	Default Accounts CORE

EXECUTION (ICS)

`T0812`	Default Credentials (ICS)
`T0883`	Internet Accessible Device (ICS)

PERSISTENCE

`T1053`	Scheduled Task/Job (IOCONTROL)
`T1543`	Create or Modify System Process (IOCONTROL)

DEFENSE EVASION

`T1027.002`	Software Packing (modified UPX)
`T1140`	Deobfuscate/Decode (AES-256-CBC config)

COMMAND AND CONTROL

`T1071.004`	DNS over HTTPS (IOCONTROL C2)
`T1071.001`	MQTT Protocol (port 8883)
`T1102`	Web Service (Telegram C2)

IMPACT

`T1491.001`	Internal Defacement (HMI splash screen)
`T1565.001`	Stored Data Manipulation (ladder logic)
`T1499`	Endpoint Denial of Service
`T0826`	Loss of Availability (ICS)
`T0828`	Loss of Productivity and Revenue (ICS)
`T0829`	Loss of View (ICS)
`T0814`	Denial of Service (ICS)

DISCOVERY

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

Kill Chain Pattern: Default Credentials to Physical Impact

Hydro Kitten's documented attack pattern follows a consistent sequence: scan for internet-exposed Unitronics PLCs on TCP port 20256, authenticate with default credentials (commonly "1111"), replace functional ladder logic with attacker-controlled code, deface HMI displays, disable upload/download capabilities, change port numbers, and apply password protection to lock out operators. In water utilities, this sequence can directly affect physical water treatment processes.

4 Tooling & Infrastructure

Custom Malware

Tool	Type	Description	First Seen
IOCONTROL	Linux Backdoor (IoT/OT)	Purpose-built Linux backdoor targeting ARM-based IoT and OT devices. Uses modified UPX packing (altered magic values to break standard UPX unpacking). Configuration encrypted with AES-256-CBC. C2 via DNS-over-HTTPS and MQTT protocol on port 8883. Also uses Telegram for C2 communication. Targets Baicells, D-Link, Hikvision, Orpak, and Teltonika devices. Initially identified as OrpraCab and QueueCat in 2023; re-emerged as IOCONTROL in 2024.	2023 (as OrpraCab); 2024 (as IOCONTROL)

Operational Techniques (PLC Exploitation)

Technique	Purpose	Source
Custom Ladder Logic Upload	Replace legitimate PLC programming with attacker-controlled logic to alter physical processes	CISA AA23-335A (2023)
HMI Defacement	Replace operator display with propaganda messages ("You have been hacked, down with Israel")	CISA AA23-335A (2023)
Firmware Downgrade	Reset PLC software to older versions to block engineering workstation compatibility	CISA AA23-335A (2023)
Port Modification	Change default port from 20256 to 20257 to prevent operator reconnection	CISA AA23-335A (2023)
Function Lockout	Disable upload/download functions; apply password protection to prevent reprogramming	CISA AA23-335A (2023)
Device Renaming	Rename PLC devices to prevent remote operator access and identification	CISA AA23-335A (2023)

Infrastructure

Category	Details	Source
Target Protocol	Unitronics PCOM protocol on TCP 20256 (default). Also TCP ports 102 (S7comm), 502 (Modbus), 44818 (EtherNet/IP).	CISA AA23-335A
C2 Channels	DNS-over-HTTPS for resolver lookups; MQTT on port 8883 (TLS-encrypted); Telegram bot API for command relay.	Claroty Team82 (Dec 2024)
Scanning	Internet-wide scanning for Unitronics PLCs; Shodan-based target identification reported.	CISA AA23-335A
Social Media	Telegram channels for propaganda, claim amplification, and operational coordination. Multiple "Mr. Soul" accounts on social platforms.	CrowdStrike Adversary Profile

5 Notable Campaigns

Early Israeli Infrastructure Claims

2020-2022

Israel · Critical Infrastructure · Disputed Claims

The CyberAv3ngers persona made multiple disputed and unverified claims of critical infrastructure compromises in Israel between 2020 and 2022. According to MITRE's G1027 entry, several of these claims were disputed or false. The persona used social media channels to amplify attack claims, consistent with the Shahid Kaveh sub-unit's mandate for "cyber-related propaganda."

C0031: Unitronics PLC Defacement Campaign

Nov 2023 - Jan 2024

United States · Ireland · Global · Water/Wastewater · Energy

The group's most well-documented campaign. CyberAv3ngers compromised at minimum 75 Unitronics Vision Series PLCs globally, including 34 or more in the U.S. water and wastewater sector. The group exploited default credentials on internet-exposed PLCs (TCP port 20256), replaced functional ladder logic, defaced HMI screens with anti-Israel messaging, and locked out operators by disabling upload/download functions and changing port numbers. In Ireland, attacks on a water utility caused service disruption for two days. This campaign triggered joint advisories from CISA, FBI, NSA, EPA, and the Israeli INCD (Advisory AA23-335A).

IOCONTROL Malware Deployment

2024

United States · Israel · IoT/OT Devices · Fuel Management

Claroty's Team82 researchers identified the IOCONTROL malware in September 2024 targeting IoT and OT devices across U.S. and Israeli critical infrastructure. The malware targeted IP cameras, routers, PLCs, HMIs, and firewalls from multiple manufacturers (Baicells, D-Link, Hikvision, Orpak, Teltonika). IOCONTROL used modified UPX packing, AES-256-CBC encrypted configuration, and communicated via DNS-over-HTTPS and MQTT (port 8883). Fuel management systems (Orpak) were among the confirmed targets. Initial detection rates were very low; by December 2024, detections had risen to 21 across AV engines.

Financial Sector Threats / Operation Epic Fury Posture

Feb-Mar 2026

United States · Western Nations · Financial Services · Banking

Following the commencement of Operation Epic Fury (February 28, 2026), CrowdStrike published a financial sector targeting advisory identifying Hydro Kitten as an explicit threat to Western financial institutions. The group issued DDoS threats against the U.S. banking sector, reportedly causing short-term disruption. CrowdStrike's Adam Meyers assessed that "much of the activity being publicized appears to be claim-driven rather than evidence-backed," suggesting the actual intrusion capability against hardened financial networks may be less developed than the group's OT/ICS capabilities.

Assessed current posture: Hydro Kitten is likely conducting DDoS and opportunistic scanning against Western financial sector targets. The group's demonstrated OT/ICS capabilities pose a more credible threat to financial sector operational technology (ATM networks, building management systems, payment processing infrastructure) than to hardened core banking systems. Financial institutions with internet-exposed Unitronics or other ICS/IoT devices are at elevated risk. [Single-source assessment per CrowdStrike advisory; independent corroboration pending.]

6 Detection & Response Recommendations

Detection Opportunities

ICS/PLC Indicators

- > Unauthorized connections to TCP port 20256 (Unitronics PCOM)
- > PLC configuration changes outside maintenance windows
- > Ladder logic file modifications or replacements
- > HMI display content changes (defacement)
- > Default port (20256) changed to non-standard ports
- > Upload/download functions disabled on PLCs

IOCONTROL Malware Indicators

- > Modified UPX-packed Linux binaries on IoT/OT devices
- > DNS-over-HTTPS traffic from OT network segments
- > MQTT connections on port 8883 from unexpected devices
- > Telegram API callbacks from IoT/OT devices
- > Unexpected processes on Linux-based ICS/IoT devices

Network Indicators

- > Scanning activity targeting Unitronics devices (TCP 20256)
- > Reconnaissance of industrial protocol ports (102, 502, 44818)
- > External connections to exposed SCADA/HMI interfaces
- > Anomalous DNS-over-HTTPS resolver traffic from OT VLANs

Financial Sector Indicators

- > DDoS traffic patterns associated with Iranian botnets
- > Scanning of payment processing or ATM management systems
- > Unauthorized access attempts to building management / HVAC controls at financial facilities
- > Exploitation attempts against IoT devices within financial network perimeters

Sample Detection Queries

Unitronics PLC Connection Monitoring (KQL)

DETECTION ONLY

```
// Detect connections to Unitronics PCOM default port
// Source: CISA Advisory AA23-335A
CommonSecurityLog
| where DestinationPort in (20256, 20257)
| where DeviceAction != "Deny"
| summarize ConnectionCount = count(),
    DistinctSources = dcount(SourceIP)
    by DestinationIP, bin(TimeGenerated, 1h)
| where ConnectionCount > 5
| sort by ConnectionCount desc
```

Context Required

TCP 20256 is the default Unitronics PCOM port. Legitimate engineering workstation connections will trigger this query. Focus on connections from unexpected source IPs or outside scheduled maintenance windows. Check port 20257 as well, since CyberAv3ngers has been documented changing default ports.

Industrial Protocol Scanning Detection (KQL)

DETECTION ONLY

```
// Detect scanning of multiple ICS protocol ports
// Ports: 20256 (Unitronics), 102 (S7comm), 502 (Modbus), 44818 (EtherNet/IP)
CommonSecurityLog
| where DestinationPort in (20256, 20257, 102, 502, 44818)
| summarize PortsScanned = dcount(DestinationPort),
    TargetCount = dcount(DestinationIP),
    Ports = make_set(DestinationPort)
    by SourceIP, bin(TimeGenerated, 15m)
| where PortsScanned >= 2 or TargetCount >= 3
| sort by TargetCount desc
```

DNS-over-HTTPS from OT Networks (KQL)

INVESTIGATION AID

```
// IOCONTROL uses DNS-over-HTTPS for C2 resolution
// Flag DoH traffic originating from OT network segments
CommonSecurityLog
| where DestinationPort == 443
| where RequestURL has_any (
    "dns.google", "cloudflare-dns.com",
    "dns.quad9.net", "doh.opendns.com"
)
| where SourceIP startswith "10.100."  // Adjust to your OT VLAN range
| summarize RequestCount = count()
    by SourceIP, RequestURL, bin(TimeGenerated, 1h)
| sort by RequestCount desc
```

Investigation Context

IOCONTROL malware uses DNS-over-HTTPS to resolve C2 infrastructure, bypassing traditional DNS monitoring. OT devices should not be making DoH queries. Any DoH traffic from ICS/OT network segments warrants immediate investigation. Adjust the SourceIP filter to match your organization's OT VLAN addressing.

MQTT C2 from IoT/OT Devices (KQL)

DETECTION ONLY

```
// IOCONTROL uses MQTT (port 8883) for C2 communication
// Monitor for unexpected MQTT connections from OT/IoT devices
CommonSecurityLog
| where DestinationPort == 8883
| where SourceIP startswith "10.100."  // Adjust to your OT VLAN range
| summarize ConnectionCount = count(),
    Destinations = make_set(DestinationIP, 10)
    by SourceIP, bin(TimeGenerated, 1h)
| sort by ConnectionCount desc
```

Priority Mitigations

1. **Remove all Unitronics PLCs from internet exposure.** If remote access is required, place behind a VPN with multi-factor authentication. This is the single highest-impact mitigation. (CISA AA23-335A)
2. **Change all default credentials** on Unitronics PLCs, HMIs, and any ICS/OT devices using factory-default passwords. The default "1111" password was the primary exploitation vector. (CISA AA23-335A)
3. **Block ICS protocol ports at the network perimeter:** TCP 20256, 102, 502, and 44818. These ports should never be accessible from the internet. (CISA AA23-335A)
4. **Upgrade Unitronics VisiLogic software to version 9.9.00 or later** and update all Vision PLC firmware to the latest available version. (CISA AA23-335A)
5. **Implement network segmentation** using the Purdue Model. Ensure OT networks are isolated from IT networks and the internet. Monitor all IT-OT boundary crossings. (CISA AA23-335A)
6. **Monitor for IOCONTROL indicators:** DNS-over-HTTPS traffic from OT segments, MQTT connections on port 8883, and Telegram API callbacks from IoT devices. (Claroty Team82)
7. **Financial sector:** Audit all IoT/OT devices within financial facility perimeters (HVAC, building management, ATM networks) for default credentials and internet exposure. (CrowdStrike advisory)

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

Unitronics default credential exploitation: Block all inbound connections to TCP ports 20256, 20257, 102, 502, and 44818 at the network perimeter. These industrial protocol ports have no legitimate reason to be internet-accessible. Safe for firewall deny rules.

IOCONTROL malware hashes: If specific SHA256 hashes become available from Claroty Team82 or other vendor reports, these are safe for hash-based blocking and EDR prevention policies. IOCONTROL is purpose-built malware with no legitimate use case.

Tier 2: Alert / Monitor (Shared Infrastructure)

DNS-over-HTTPS resolvers: IOCONTROL uses public DoH resolvers (dns.google, cloudflare-dns.com) for C2 infrastructure resolution. Blocking these resolvers entirely may disrupt legitimate services. Recommend alerting on DoH traffic from OT/IoT network segments specifically, not blocking DoH globally.

MQTT broker IPs: IOCONTROL communicates via MQTT on port 8883. Public MQTT brokers are used by many legitimate IoT applications. Alert on MQTT connections from OT segments to unexpected destinations. Do NOT block port 8883 globally.

Tier 3: Investigate (Unconfirmed)

Financial sector DDoS source IPs: DDoS source IPs associated with Hydro Kitten financial sector threats have not been publicly released. Any DDoS traffic targeting financial infrastructure should be investigated using standard DDoS mitigation procedures. Do not add IPs to permanent block lists based solely on DDoS participation, as they may be compromised residential devices.

Telegram C2 endpoints: IOCONTROL uses Telegram bot API for C2 communication. Blocking Telegram entirely may affect legitimate business communications. Investigate Telegram API traffic from IoT/OT devices specifically.

Network Indicators (Ports)

Indicator	Type	Context	Source	Confidence
`TCP/20256`	Port	Unitronics PCOM default port; primary exploitation vector	CISA AA23-335A	High
`TCP/20257`	Port	Modified port used by CyberAv3ngers after compromise	CISA AA23-335A	High
`TCP/8883`	Port	MQTT TLS; IOCONTROL C2 channel	Claroty Team82 (Dec 2024)	High

Default Credentials Exploited

Indicator	Context	Source	Confidence
`1111` (default password)	Unitronics Vision Series PLC default password; primary exploitation vector in C0031 campaign	CISA AA23-335A	High

HMI Defacement String

Indicator	Context	Source	Confidence
`You have been hacked, down with Israel`	Splash screen message deployed on defaced Unitronics HMIs	CISA AA23-335A; multiple incident reports	High

IOC Limitations

Specific IP addresses, file hashes (SHA256), and C2 domains for Hydro Kitten / CyberAv3ngers operations have been removed from the CISA advisory as "outdated" per the December 2024 update. Historical IOCs are available in the original advisory PDFs. For IOCONTROL malware hashes, security teams should obtain indicators directly from Claroty Team82's research publications. Financial sector-specific IOCs have not been published by CrowdStrike at time of writing.

B Appendix B: References

Government Advisories & Standards Bodies

[1] **CISA, FBI, NSA, EPA, Israel INCD** - "IRGC-Affiliated Cyber Actors Exploit PLCs in Multiple Sectors, Including U.S. Water and Wastewater Systems Facilities" (Advisory AA23-335A, December 2023; updated December 2024)
cisa.gov

[2] **MITRE ATT&CK** - "Group G1027: CyberAv3ngers, Soldiers of Solomon"
attack.mitre.org

[3] **U.S. Department of the Treasury** - "Treasury Designates IRGC-CEC Officials for Cyber Operations Against U.S. Critical Infrastructure" (February 2024)
home.treasury.gov

Vendor Threat Intelligence (Primary)

[4] **CrowdStrike** - "Hydro Kitten Adversary Profile"
crowdstrike.com

[5] **CrowdStrike** - Hydro Kitten financial sector targeting advisory, accessed March 11, 2026

[6] **CrowdStrike** - "2026 Global Threat Report" (February 2026)
crowdstrike.com

[7] **Claroty Team82** - IOCONTROL malware analysis (December 2024)
claroty.com

[8] **Armis** - "IOControl Malware: What's New, What's Not?" (2025)
armis.com

[9] **Trellix** - "The Iranian Cyber Capability 2026"
trellix.com

Investigative Journalism & Incident Reporting

[10] **SecurityWeek** - "Iranian Hackers Use IOCONTROL Malware to Target OT, IoT Devices in US, Israel"
securityweek.com

[11] **SecurityWeek** - "Iran Cyber Front: Hacktivist Activity Rises, but State-Sponsored Attacks Stay Low"
securityweek.com

[12] **American Banker** - "War in Iran brings cyber frontline to U.S. banks" (March 2026)
americanbanker.com

[13] **The Hacker News** - "Iran-Linked IOCONTROL Malware Targets SCADA and Linux-Based IoT Platforms" (December 2024)
thehackernews.com

[14] **Axios** - "Iranian cyber attacks: What to know about U.S., Israel's cyberwarfare" (March 2026)
axios.com

OSINT & Analyst Research

[15] **SecurityWeek** - "Leaked Files From Offensive Cyber Unit Show Iran's Interest in Targeting ICS"
securityweek.com

[16] **CSIS** - "Beyond Hacktivism: Iran's Coordinated Cyber Threat Landscape"
csis.org

[17] **SOCRadar** - "Dark Web Profile: Cyber Av3ngers"
socradar.io

[18] **Flashpoint** - "IOCONTROL Malware: A New Threat Targeting Critical Infrastructure"
flashpoint.io

[19] **Intruvent Technologies** - "INT-GSR-2026-IRANCONFLICT-v1.2 / v1.3" (Iran Conflict SITREP series, 2026)

TRACK THIS THREAT ACTOR CONTINUOUSLY

BRACE monitors Hydro Kitten 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