INTRUVENT

COMPREHENSIVE THREAT HUNTING GUIDE

Hydro Kitten: Financial Sector Targeting and ICS/IoT Intrusion Detection

Detecting IRGC-CEC operations against financial infrastructure, hunting for IOCONTROL malware, and identifying Unitronics PLC exploitation

Version 1.0
Published March 18, 2026
Threat Actor Hydro Kitten / CyberAv3ngers (IRGC-CEC)
Classification TLP:CLEAR
Total Hunt Time 4 Hours
Target Sectors Financial Services, Water/Wastewater, Energy, Critical Infrastructure

Intruvent Technologies
INT-THG-2026-HYDROKITTEN-FIN-v1.0

Table of Contents

Overview

Executive Summary 3
MITRE ATT&CK Mapping 4

Hunt Modules

Module 1: Internet-Exposed ICS/IoT Device Discovery 5
Module 2: Unitronics PLC Default Credential Exploitation 6
Module 3: IOCONTROL Malware Detection on Linux IoT/OT Devices 7
Module 4: DNS-over-HTTPS C2 Channel Detection 8
Module 5: MQTT C2 Communication from OT Segments 9
Module 6: PLC Ladder Logic and Configuration Tampering 10
Module 7: Financial Facility OT/IoT Asset Audit 11
Module 8: DDoS Precursor and Volumetric Attack Detection 12
Module 9: Telegram Bot API C2 from IoT Devices 13
Module 10: Industrial Protocol Scanning Detection 14

Appendices

Appendix A: Indicators of Compromise 15
Appendix B: Detection Rules 17
Appendix C: References 19

1 Executive Summary

AT A GLANCE

THREAT ACTOR Hydro Kitten / CyberAv3ngers (IRGC-CEC, Iran)	PRIMARY OBJECTIVE ICS/OT disruption; financial sector targeting (new)
ACTIVE SINCE 2020 (propaganda); 2023 (confirmed ICS compromise)	TARGET SECTORS Financial Services, Water/Wastewater, Energy, Healthcare
KEY DIFFERENTIATOR ICS/IoT-focused group expanding to financial sector	CUSTOM MALWARE IOCONTROL (Linux IoT/OT backdoor)

Hydro Kitten (CrowdStrike designation; also tracked as CyberAv3ngers, BAUXITE by Dragos, G1027 by MITRE) is an IRGC-CEC threat actor attributed to the Shahid Kaveh sub-unit. The group is best known for its November 2023 campaign against Unitronics Vision Series PLCs in water/wastewater facilities across the United States and Ireland (MITRE Campaign C0031). In 2024, the group deployed IOCONTROL, a purpose-built Linux backdoor targeting IoT and OT devices across multiple manufacturers.

In March 2026, CrowdStrike published a financial sector targeting advisory identifying Hydro Kitten as an explicit threat to Western financial institutions, coinciding with the escalation of the U.S.-Israel-Iran conflict (Operation Epic Fury). CrowdStrike's Adam Meyers assessed that much of the publicized financial sector activity appears "claim-driven rather than evidence-backed." The group's demonstrated ICS/OT capabilities remain its most credible threat vector against the financial sector, particularly against operational technology within financial facilities (building management systems, HVAC, ATM networks, and payment processing infrastructure with embedded IoT components).

This guide provides **10 hunt modules** designed to help defenders: (1) identify internet-exposed ICS/IoT devices vulnerable to Hydro Kitten exploitation, (2) detect IOCONTROL malware and its C2 channels, (3) hunt for Unitronics PLC exploitation indicators, (4) audit financial facility OT/IoT assets, and (5) detect DDoS precursors and reconnaissance activity. Total estimated hunt time is **4 hours**.

Threat Overview

Hydro Kitten operates at the intersection of traditional IT network attacks and operational technology (OT) targeting. The group's documented kill chain begins with internet scanning for exposed Unitronics PLCs, authenticates with default credentials (commonly "1111"), then replaces functional ladder logic with attacker-controlled code. In water utilities, this sequence can directly affect physical treatment processes. The 2023 Ireland attack caused a two-day water service disruption.

The IOCONTROL malware (identified in 2024) demonstrated a more sophisticated capability. This Linux backdoor targets ARM-based IoT and OT devices from multiple manufacturers (Baicells, D-Link, Hikvision, Orpak, Teltonika). It uses modified UPX packing to evade analysis, encrypts its configuration with AES-256-CBC, and communicates via DNS-over-HTTPS, MQTT (port 8883), and Telegram. Fuel management systems (Orpak) were among confirmed targets.

The financial sector expansion announced by CrowdStrike in March 2026 warrants defensive attention. Financial institutions should focus their hunting on two vectors: (1) internet-exposed OT/IoT devices within their physical facilities and network perimeters, and (2) DDoS targeting of customer-facing services. The group's demonstrated PLC exploitation capabilities could theoretically affect building management systems, HVAC controls, and physical security systems at financial facilities.

KEY CHARACTERISTICS

- IRGC-CEC state-sponsored (Shahid Kaveh)
- ICS/OT disruption specialist
- IOCONTROL Linux IoT/OT backdoor
- Unitronics PLC default credential exploitation
- DNS-over-HTTPS C2 channel
- MQTT protocol C2 (port 8883)
- Telegram bot API for command relay
- HMI defacement as propaganda
- Financial sector targeting (new, 2026)
- 6 officials sanctioned (U.S. Treasury)

Source Limitation Notice
Hydro Kitten has limited public documentation compared to established Iranian APT groups. The financial sector targeting advisory from CrowdStrike (March 2026) is single-source reporting. Modules 7 and 8 (financial facility OT audit and DDoS detection) are based on assessed threat vectors rather than confirmed intrusion TTPs. Gaps are marked with [REQUIRES VERIFICATION] throughout.

2 MITRE ATT&CK Mapping

The following techniques are documented for the CyberAv3ngers cluster (MITRE G1027) and IOCONTROL malware operations. Sources: MITRE ATT&CK, CISA AA23-335A, Claroty Team82.

`T1078.001` CORE **Default Accounts** Primary initial access vector; exploitation of default credentials ("1111") on Unitronics PLCs	`T1190` **Exploit Public-Facing Application** Internet-exposed Unitronics PLCs on TCP 20256; IOCONTROL targeting exposed IoT devices	`T1027.002` **Software Packing** IOCONTROL uses modified UPX packing with altered magic values to frustrate analysis
`T1071.004` **Application Layer Protocol: DNS** IOCONTROL uses DNS-over-HTTPS to resolve C2 infrastructure, bypassing traditional DNS monitoring	`T1071.001` **Application Layer Protocol: Web Protocols** MQTT protocol on port 8883 (TLS) for IOCONTROL C2 communication	`T1102` **Web Service** Telegram bot API used by IOCONTROL for command relay
`T1565.001` **Stored Data Manipulation** Replaced PLC ladder logic; modified firmware versions; altered port configurations	`T1491.001` **Internal Defacement** Replaced HMI display with propaganda: "You have been hacked, down with Israel"	`T1499` **Endpoint Denial of Service** Disabled PLC upload/download functions; changed ports to prevent operator reconnection
`T0812 (ICS)` **Default Credentials** Exploited default password "1111" on Unitronics Vision Series PLCs	`T0883 (ICS)` **Internet Accessible Device** Targeted internet-connected PLCs and cellular modems in OT networks	`T0826 (ICS)` **Loss of Availability** Rendered PLC/HMI systems unavailable; Ireland water utility offline for two days

3 Hunt Modules

1 Internet-Exposed ICS/IoT Device Discovery

Duration: 30 min Priority: CRITICAL

Objective: Identify any internet-exposed ICS, IoT, or OT devices within the organization's perimeter that could be targeted by Hydro Kitten's documented exploitation techniques.

Background

Hydro Kitten's primary attack vector is the exploitation of internet-accessible ICS/IoT devices. The group scans for Unitronics PLCs on TCP 20256 and deploys IOCONTROL against a range of Linux-based IoT devices. Financial institutions should audit for unexpected internet exposure of building management systems, HVAC controllers, physical security systems, and any IoT devices with embedded Linux.

Hunt Procedure: External Attack Surface Scan

INVESTIGATION AID

BASH (NMAP)

```bash
# Scan your external IP ranges for exposed ICS/IoT ports
# Ports: 20256 (Unitronics), 102 (S7comm), 502 (Modbus),
#        44818 (EtherNet/IP), 8883 (MQTT TLS), 1883 (MQTT)
# IMPORTANT: Only scan IP ranges you own or have authorization for
nmap -sS -p 20256,20257,102,502,44818,8883,1883 \
    --open -oN ics_exposure_scan.txt \
    YOUR_EXTERNAL_IP_RANGES
```

Hunt Procedure: Firewall Rule Audit (KQL)

DETECTION ONLY

KQL (AZURE FIREWALL / NSG)

```
// Identify any firewall rules permitting inbound traffic to ICS ports
// These ports should NEVER be internet-accessible
AzureNetworkAnalytics_CL
| where FlowDirection_s == "I"  // Inbound
| where DestPort_d in (20256, 20257, 102, 502, 44818)
| where FlowStatus_s == "A"  // Allowed
| summarize ConnectionCount = count()
    by DestPort_d, DestIP_s, SrcIP_s, NSGRule_s
| sort by ConnectionCount desc
```

- ☐ Run external port scan against all organization-owned IP ranges for ICS/IoT ports
- ☐ Audit cloud firewall rules and NSG configurations for permitted ICS protocol traffic
- ☐ Inventory all Unitronics devices; verify none are internet-accessible
- ☐ Check for Baicells, D-Link, Hikvision, Orpak, and Teltonika devices (IOCONTROL targets)
- ☐ Document all findings; any internet-exposed ICS/IoT device is a critical finding

Critical: Any Exposed ICS Device Requires Immediate Action
CISA Advisory AA23-335A explicitly states: take all Unitronics PLCs off the internet. Any internet-exposed ICS or IoT device within the organization's perimeter should be immediately isolated and placed behind VPN/firewall controls. This is the single highest-impact mitigation against Hydro Kitten.

2 Unitronics PLC Default Credential Exploitation

Duration: 20 min Priority: CRITICAL

Objective: Detect exploitation attempts against Unitronics PLCs using default credentials and identify post-compromise indicators (port changes, firmware downgrades, ladder logic replacement).

Hunt Procedure: Unitronics Connection Monitoring

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect connections to Unitronics PCOM ports from unexpected sources
// Source: CISA Advisory AA23-335A
CommonSecurityLog
| where DestinationPort in (20256, 20257)
| where DeviceAction != "Deny"
| where not(SourceIP startswith "10." or SourceIP startswith "192.168."
    or SourceIP startswith "172.16.")  // Exclude internal
| summarize ConnectionCount = count(),
    FirstSeen = min(TimeGenerated),
    LastSeen = max(TimeGenerated)
    by SourceIP, DestinationIP, DestinationPort
| sort by ConnectionCount desc
```

Context
Any external connection to TCP 20256 or 20257 targeting a Unitronics device is suspicious. Legitimate engineering connections should originate from known internal engineering workstations only. CyberAv3ngers changed the default port from 20256 to 20257 post-compromise; monitor both ports.

Manual Verification Steps

- Log into each Unitronics PLC and verify the password is not the factory default "1111"
- Check VisiLogic software version; confirm it is 9.9.00 or later
- Verify PCOM port is set to 20256 (not modified to 20257 or other non-standard port)
- Review ladder logic for unauthorized modifications
- Check HMI display content for defacement indicators
- Verify upload/download functions are enabled (not locked by attacker)

- ☐ Audit all Unitronics PLCs for default credential usage
- ☐ Verify firmware and VisiLogic software versions are current
- ☐ Check for port modifications (20256 changed to 20257 or other)
- ☐ Review ladder logic integrity against known-good backups
- ☐ Confirm HMI displays show expected content

3 IOCONTROL Malware Detection on Linux IoT/OT Devices

Duration: 30 min Priority: CRITICAL

Objective: Detect indicators of IOCONTROL malware on Linux-based IoT and OT devices, including modified UPX-packed binaries, AES-256-CBC encrypted configurations, and suspicious process activity.

Background

IOCONTROL is a purpose-built Linux backdoor targeting ARM-based IoT and OT devices. It uses modified UPX packing (altered magic values that break standard UPX unpacking utilities), encrypts its configuration with AES-256-CBC, and communicates via DNS-over-HTTPS, MQTT (port 8883), and Telegram bot API. The malware was initially identified as OrpraCab and QueueCat in 2023 before re-emerging as IOCONTROL in 2024. Confirmed target devices include products from Baicells, D-Link, Hikvision, Orpak, and Teltonika.

Hunt Procedure: Suspicious Binaries on Linux IoT/OT

INVESTIGATION AID

BASH (LINUX - RUN ON IOT/OT DEVICES)

```bash
# Search for UPX-packed binaries with modified magic values
# IOCONTROL modifies UPX magic bytes to avoid detection
# Run on each Linux IoT/OT device accessible via SSH

# 1. Find recently modified executable files
find / -type f -executable -newer /etc/hostname -mtime -90 2>/dev/null

# 2. Check for UPX-packed binaries (look for "UPX!" magic bytes)
# Modified IOCONTROL samples alter these bytes
find / -type f -executable -exec sh -c \
    'hexdump -C "$1" | head -50 | grep -qi "upx"' _ {} \; -print 2>/dev/null

# 3. Check for unexpected cron jobs or systemd services
crontab -l 2>/dev/null
ls -la /etc/cron.d/ /etc/systemd/system/ 2>/dev/null | grep -v ".wants"

# 4. Check for unexpected outbound connections
ss -tunp | grep -E ":(443|8883|20256)" 2>/dev/null
```

Hunt Procedure: IOCONTROL Network Indicators

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect potential IOCONTROL C2 patterns from OT network segments
// IOCONTROL uses: DNS-over-HTTPS, MQTT (8883), Telegram API
// Source: Claroty Team82 (December 2024)
CommonSecurityLog
| where SourceIP startswith "10.100."  // Adjust to your OT VLAN
| where (
    // DNS-over-HTTPS to public resolvers
    (DestinationPort == 443 and RequestURL has_any (
        "dns.google", "cloudflare-dns.com", "dns.quad9.net"))
    or
    // MQTT TLS connections
    (DestinationPort == 8883)
    or
    // Telegram Bot API
    (RequestURL has "api.telegram.org")
)
| summarize EventCount = count(),
    Protocols = make_set(DestinationPort)
    by SourceIP, bin(TimeGenerated, 1h)
| sort by EventCount desc
```

- ☐ Inventory all Linux-based IoT/OT devices (cameras, routers, PLCs, gateways)
- ☐ Check each device for unexpected executables or modified system binaries
- ☐ Review cron jobs and systemd services for persistence mechanisms
- ☐ Monitor network traffic from OT segments for DoH, MQTT, and Telegram callbacks
- ☐ Compare device firmware hashes against vendor-provided known-good hashes

IOCONTROL Hash Availability
Specific SHA256 hashes for IOCONTROL samples should be obtained from Claroty Team82's research publications. By December 2024, detection rates had risen to 21 across AV engines, up from near-zero in September 2024. Contact your threat intelligence vendor for current IOCs.

4 DNS-over-HTTPS C2 Channel Detection

Duration: 20 min Priority: HIGH

Objective: Detect IOCONTROL's use of DNS-over-HTTPS for C2 infrastructure resolution, focusing on DoH traffic from OT and IoT network segments where such traffic is anomalous.

Background

IOCONTROL uses DNS-over-HTTPS (DoH) to resolve its C2 server addresses, bypassing traditional DNS monitoring that organizations rely on for threat detection. OT and IoT devices have no legitimate reason to perform DoH queries. Any DoH traffic from OT network segments is a high-fidelity detection signal.

Hunt Procedure: DoH Traffic from OT Segments

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect DNS-over-HTTPS queries from OT/IoT network segments
// OT devices should NOT be making DoH queries
// Source: Claroty Team82 IOCONTROL analysis
let DoH_Providers = dynamic([
    "dns.google", "cloudflare-dns.com", "dns.quad9.net",
    "doh.opendns.com", "dns.adguard.com", "doh.dns.sb"
]);
CommonSecurityLog
| where DestinationPort == 443
| where RequestURL has_any (DoH_Providers)
    or DestinationIP in (
        "8.8.8.8", "8.8.4.4",        // Google DNS
        "1.1.1.1", "1.0.0.1",        // Cloudflare DNS
        "9.9.9.9", "149.112.112.112"  // Quad9
    )
| where SourceIP startswith "10.100."  // Adjust to OT VLAN
| summarize QueryCount = count(),
    FirstSeen = min(TimeGenerated),
    LastSeen = max(TimeGenerated)
    by SourceIP, DestinationIP
| sort by QueryCount desc
```

Hunt Procedure: Splunk (Network Traffic)

DETECTION ONLY

SPL (SPLUNK)

```
| Detect DoH traffic from OT network segments
index=firewall sourcetype=pan:traffic dest_port=443
    (dest_ip="8.8.8.8" OR dest_ip="8.8.4.4"
     OR dest_ip="1.1.1.1" OR dest_ip="1.0.0.1"
     OR dest_ip="9.9.9.9" OR dest_ip="149.112.112.112")
    src_ip="10.100.*"
| stats count as connection_count
    earliest(_time) as first_seen
    latest(_time) as last_seen
    by src_ip, dest_ip
| sort -connection_count
```

- ☐ Query firewall and proxy logs for DoH traffic from OT/IoT VLANs
- ☐ Identify all source IPs making DoH queries from OT segments
- ☐ Cross-reference source IPs with IoT/OT device inventory
- ☐ Any DoH traffic from an OT device warrants immediate investigation

5 MQTT C2 Communication from OT Segments

Duration: 20 min Priority: HIGH

Objective: Detect IOCONTROL's use of MQTT protocol (port 8883, TLS-encrypted) for C2 communication from IoT/OT devices.

Background

MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol commonly used in IoT environments. IOCONTROL uses MQTT on port 8883 (TLS-encrypted) for C2 communication. While MQTT is legitimate in some IoT deployments, unexpected MQTT connections from devices that do not normally use this protocol, or MQTT connections to unknown external brokers, are suspicious indicators.

Hunt Procedure: MQTT Connections from OT Devices

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect MQTT connections from OT/IoT network segments
// Port 8883 = MQTT over TLS; Port 1883 = MQTT plaintext
CommonSecurityLog
| where DestinationPort in (8883, 1883)
| where SourceIP startswith "10.100."  // Adjust to OT VLAN
| summarize ConnectionCount = count(),
    DistinctDestinations = dcount(DestinationIP),
    Destinations = make_set(DestinationIP, 10)
    by SourceIP, DestinationPort, bin(TimeGenerated, 1h)
| sort by ConnectionCount desc
```

Triage Steps

- Identify which OT/IoT devices are making MQTT connections
- Determine if MQTT is an expected protocol for each device (some IoT sensors use MQTT legitimately)
- Check destination IPs against known IoT cloud platforms (e.g., AWS IoT, Azure IoT Hub)
- Unknown or unexpected MQTT broker destinations from OT devices warrant forensic investigation

- ☐ Inventory all devices that legitimately use MQTT in OT/IoT segments
- ☐ Baseline expected MQTT broker destinations
- ☐ Flag any MQTT connections to unknown external brokers
- ☐ Investigate any new MQTT traffic from devices not previously using this protocol

6 PLC Ladder Logic and Configuration Tampering

Duration: 30 min Priority: CRITICAL

Objective: Detect unauthorized modifications to PLC ladder logic, firmware versions, and configuration parameters that match CyberAv3ngers' documented post-compromise behavior.

Background

After gaining access to Unitronics PLCs, CyberAv3ngers performed several documented post-compromise actions: replaced functional ladder logic with attacker-controlled code, downgraded firmware to older versions, changed the default PCOM port (20256 to 20257), disabled upload/download capabilities, applied password protection, and renamed devices. These actions are designed to lock out operators and prevent recovery.

Hunt Procedure: Configuration Change Detection

INVESTIGATION AID

MANUAL VERIFICATION CHECKLIST

```
# For each Unitronics PLC in the environment:

# 1. CREDENTIAL CHECK
# - Can you authenticate with default password "1111"?
# - If YES: credential is unchanged = vulnerable = CRITICAL

# 2. PORT CHECK
# - Is PCOM listening on 20256 (expected) or 20257 (post-compromise)?
# - Any non-standard port = potential compromise indicator

# 3. FIRMWARE CHECK
# - Compare current firmware version against expected version
# - Downgraded firmware = potential compromise indicator

# 4. LADDER LOGIC INTEGRITY
# - Compare current ladder logic against known-good backup
# - Any unauthorized modification = CRITICAL

# 5. FUNCTION CHECK
# - Can you upload/download programs? If disabled = compromise indicator
# - Is password protection applied that was not configured by operators?

# 6. DEVICE NAME CHECK
# - Has the device name been changed from its expected designation?

# 7. HMI DISPLAY CHECK
# - Does the HMI show expected operational displays?
# - Defacement message: "You have been hacked, down with Israel"
```

- ☐ Verify ladder logic integrity against known-good backups on all PLCs
- ☐ Confirm firmware versions match expected versions (check for downgrades)
- ☐ Test default credentials on all Unitronics devices (any success = critical vulnerability)
- ☐ Verify PCOM port settings on all Unitronics PLCs
- ☐ Check upload/download function status on each PLC
- ☐ Review HMI displays for unauthorized content

7 Financial Facility OT/IoT Asset Audit

Duration: 30 min Priority: HIGH

Objective: Identify and audit OT and IoT devices within financial facility perimeters that could serve as entry points for Hydro Kitten's ICS/OT exploitation capabilities.

Assessed Threat Vector
This module addresses an assessed (not confirmed) threat vector. Hydro Kitten's financial sector targeting has been identified by CrowdStrike, but specific intrusion TTPs against financial institution OT/IoT assets have not been publicly documented. This module applies the group's demonstrated ICS/OT exploitation capabilities to the financial sector context. [REQUIRES VERIFICATION: No public reports of Hydro Kitten compromising financial facility OT systems.]

Financial Facility OT/IoT Inventory

Financial institutions commonly operate OT and IoT devices that may be vulnerable to Hydro Kitten's demonstrated capabilities. Audit the following device categories:

Device Category	Risk Context	Audit Priority
Building Management Systems (BMS)	HVAC, lighting, elevator controls; often Linux-based; may use Modbus/BACnet	High
Physical Security Systems	IP cameras (Hikvision, D-Link), access control, alarm systems	High
ATM Networks	Embedded systems; network connectivity to core banking; potential lateral movement path	Critical
UPS / Power Management	Network-connected UPS devices; often have web interfaces with default credentials	Medium
Data Center HVAC / Environmental	Environmental monitoring sensors; cooling controls; some use PLCs	Medium

Hunt Procedure: Default Credential Sweep

INVESTIGATION AID

MANUAL PROCESS

```
# For each OT/IoT device category in the financial facility:
#
# 1. Obtain complete inventory from facilities management team
# 2. For each device, check:
#    - Is the device internet-accessible? (CRITICAL if yes)
#    - Are default credentials still in use?
#    - Is firmware up to date?
#    - Is the device on a segmented network (separate from IT)?
#    - Are management interfaces restricted to authorized IPs?
#
# 3. Common default credentials to test:
#    Unitronics: "1111"
#    Hikvision: admin/12345
#    D-Link: admin/(blank)
#    Generic: admin/admin, admin/password, root/root
```

- ☐ Obtain full OT/IoT device inventory from facilities management
- ☐ Verify network segmentation between OT/IoT and corporate IT networks
- ☐ Test all devices for default credential usage
- ☐ Confirm no OT/IoT devices are internet-exposed
- ☐ Check IP camera systems for Hikvision devices (IOCONTROL target)
- ☐ Review firmware versions on all OT/IoT devices

8 DDoS Precursor and Volumetric Attack Detection

Duration: 20 min Priority: MEDIUM

Objective: Detect DDoS reconnaissance and volumetric attacks targeting financial sector services, consistent with Hydro Kitten's documented DDoS threat claims against U.S. banking infrastructure.

Claim-Driven Threat
CrowdStrike's Adam Meyers assessed that Hydro Kitten's DDoS claims appear "claim-driven rather than evidence-backed." This module addresses a real but potentially overstated threat vector. DDoS is the lowest-sophistication attack available to the group and the most likely financial sector attack type.

Hunt Procedure: DDoS Precursor Detection

DETECTION ONLY

KQL (AZURE DDOS PROTECTION / WAF)

```
// Detect volumetric traffic spikes against public-facing services
// Financial sector: web banking, API gateways, payment portals
AzureDiagnostics
| where Category == "DDoSProtectionNotifications"
    or Category == "DDoSMitigationReports"
| where TimeGenerated > ago(7d)
| project TimeGenerated, Resource, properties_s
| sort by TimeGenerated desc
```

Hunt Procedure: Anomalous Traffic Volume

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Baseline and detect anomalous request volumes
// Adjust ResourceUri to your public-facing financial services
AzureMetrics
| where ResourceId has "publicIPAddresses"
| where MetricName == "IfUnderDDoSAttack"
| where Maximum > 0
| project TimeGenerated, ResourceId, Maximum
| sort by TimeGenerated desc
```

- ☐ Review DDoS protection alerts for the past 30 days
- ☐ Verify DDoS mitigation is enabled on all public-facing financial services
- ☐ Confirm rate limiting is configured on API gateways and web application firewalls
- ☐ Review CDN/WAF logs for volumetric anomalies
- ☐ Ensure incident response playbook includes DDoS escalation procedures

9 Telegram Bot API C2 from IoT Devices

Duration: 15 min Priority: HIGH

Objective: Detect IOCONTROL's use of Telegram bot API for C2 command relay from compromised IoT/OT devices.

Hunt Procedure: Telegram API Callbacks from OT Devices

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect Telegram Bot API connections from OT/IoT network segments
// IoT/OT devices should NOT be contacting Telegram
CommonSecurityLog
| where RequestURL has "api.telegram.org"
    or DestinationHostName has "api.telegram.org"
| where SourceIP startswith "10.100."  // Adjust to OT VLAN
| summarize CallbackCount = count(),
    FirstSeen = min(TimeGenerated),
    LastSeen = max(TimeGenerated)
    by SourceIP, DestinationIP
| sort by CallbackCount desc
```

Hunt Procedure: Splunk Variant

DETECTION ONLY

SPL (SPLUNK)

```
index=proxy OR index=firewall
    (url="*api.telegram.org*" OR dest="149.154.167.*")
    src_ip="10.100.*"
| stats count as callback_count
    earliest(_time) as first_seen
    latest(_time) as last_seen
    by src_ip, dest_ip
| sort -callback_count
```

- ☐ Query proxy and firewall logs for Telegram API traffic from OT/IoT segments
- ☐ Any Telegram API callback from an OT/IoT device is a high-confidence compromise indicator
- ☐ Cross-reference source IPs with device inventory
- ☐ Consider blocking Telegram API endpoints from OT network segments at the firewall

10 Industrial Protocol Scanning Detection

Duration: 15 min Priority: HIGH

Objective: Detect external scanning and reconnaissance of industrial protocol ports targeting the organization's network perimeter, consistent with Hydro Kitten's documented internet-wide scanning for vulnerable ICS devices.

Hunt Procedure: Inbound ICS Protocol Scanning

DETECTION ONLY

KQL (MICROSOFT SENTINEL)

```
// Detect external scanning of ICS/OT protocol ports
// Source: CISA AA23-335A; CyberAv3ngers known scanning targets
let ICS_Ports = dynamic([20256, 20257, 102, 502, 44818, 2222, 4840]);
CommonSecurityLog
| where DestinationPort in (ICS_Ports)
| where not(SourceIP startswith "10." or SourceIP startswith "192.168."
    or SourceIP startswith "172.16.")
| summarize ScanCount = count(),
    PortsTargeted = make_set(DestinationPort),
    TargetIPs = dcount(DestinationIP)
    by SourceIP, bin(TimeGenerated, 1h)
| where ScanCount > 10
| sort by ScanCount desc
```

Hunt Procedure: Splunk Variant

DETECTION ONLY

SPL (SPLUNK)

```
index=firewall sourcetype=pan:traffic direction=inbound
    (dest_port=20256 OR dest_port=20257 OR dest_port=102
     OR dest_port=502 OR dest_port=44818)
    NOT (src_ip="10.*" OR src_ip="192.168.*" OR src_ip="172.16.*")
| stats count as scan_count
    dc(dest_ip) as targets
    values(dest_port) as ports_targeted
    by src_ip
| where scan_count > 10
| sort -scan_count
```

- ☐ Query perimeter firewall logs for inbound connections to ICS protocol ports
- ☐ Identify and document all scanning source IPs
- ☐ Cross-reference scanner IPs with threat intelligence feeds
- ☐ Verify all ICS protocol ports are blocked at the perimeter (any allowed = critical gap)
- ☐ Report persistent scanners to ISP abuse contacts and relevant ISACs

A Appendix A: Indicators of Compromise

Blocking Guidance: 3-Tier IOC Classification

Tier 1: Block (High Confidence)

Inbound ICS protocol ports: Block all inbound connections to TCP 20256, 20257, 102, 502, and 44818 at the network perimeter. No legitimate reason for these to be internet-accessible. Safe for firewall deny rules.

IOCONTROL malware hashes: When specific SHA256 hashes are obtained from Claroty Team82, these are safe for EDR prevention policies. IOCONTROL has no legitimate use case.

Tier 2: Alert / Monitor (Shared Infrastructure)

DoH resolvers (dns.google, cloudflare-dns.com, etc.): Blocking these globally may disrupt legitimate services. Alert on DoH traffic from OT/IoT VLANs specifically. Consider blocking DoH from OT segments only.

MQTT brokers (port 8883): Legitimate IoT applications use MQTT. Alert on MQTT from devices not baselined for MQTT usage. Do NOT block port 8883 globally.

Telegram API (api.telegram.org): Blocking Telegram may affect legitimate business use. Alert on Telegram traffic from OT/IoT segments. Consider blocking from OT VLANs.

Tier 3: Investigate (Unconfirmed)

DDoS source IPs: DDoS traffic against financial services may originate from compromised residential devices or botnets. Do not add DDoS source IPs to permanent block lists; use rate limiting and DDoS mitigation services instead.

Financial sector IOCs: CrowdStrike has not published specific IOCs for Hydro Kitten financial sector operations. If financial-sector-specific indicators become available, classify per this framework before deploying.

Network Indicators

Indicator	Type	Context	Source	Tier
`TCP/20256`	Port	Unitronics PCOM default; primary exploitation target	CISA AA23-335A	Block
`TCP/20257`	Port	Modified Unitronics port (post-compromise indicator)	CISA AA23-335A	Block
`TCP/102`	Port	S7comm (Siemens); ICS protocol port	CISA AA23-335A	Block
`TCP/502`	Port	Modbus; ICS protocol port	CISA AA23-335A	Block
`TCP/44818`	Port	EtherNet/IP; ICS protocol port	CISA AA23-335A	Block
`TCP/8883`	Port	MQTT TLS; IOCONTROL C2 channel	Claroty Team82	Alert

Behavioral Indicators

Indicator	Context	Source
HMI defacement: `"You have been hacked, down with Israel"`	Splash screen message on compromised Unitronics PLCs	CISA AA23-335A; incident reports
Default password `"1111"` on Unitronics PLCs	Vulnerability indicator; primary exploitation vector	CISA AA23-335A
DNS-over-HTTPS from OT/IoT devices	IOCONTROL C2 resolution method; OT devices should not use DoH	Claroty Team82
Telegram API callbacks from OT/IoT devices	IOCONTROL C2 channel; OT devices should not contact Telegram	Claroty Team82
Modified UPX-packed Linux binaries on IoT/OT	IOCONTROL uses UPX with altered magic values	Claroty Team82

IOC Availability Note
Specific IP addresses and file hashes for CyberAv3ngers/Hydro Kitten operations have been removed from the CISA advisory as "outdated" per the December 2024 update. Historical IOCs are available in the original AA23-335A PDF. For IOCONTROL malware hashes, obtain indicators directly from Claroty Team82 publications. Financial sector IOCs have not been published at time of writing.

B Appendix B: Detection Rules

Detection Rule Disclaimer
The following detection rules are provided as starting points for threat hunting. They require tuning to each organization's environment, network architecture, and OT/IoT device inventory. All rules should be tested in a non-production environment before deployment. OT VLAN ranges (shown as "10.100.*") must be adjusted to match your organization's network addressing.

Rule 1: ICS Port Exposure Alert

Inbound ICS Protocol Traffic Allowed KQL

BLOCKING SAFE

```
// ALERT: Inbound traffic to ICS ports was ALLOWED through firewall
// Any match = ICS port is internet-exposed = CRITICAL vulnerability
CommonSecurityLog
| where DestinationPort in (20256, 20257, 102, 502, 44818)
| where DeviceAction in ("Allow", "Permit", "Accept")
| where not(SourceIP startswith "10." or SourceIP startswith "192.168.")
| project TimeGenerated, SourceIP, DestinationIP, DestinationPort,
    DeviceAction, DeviceName
```

Rule 2: OT Segment DoH Activity

DNS-over-HTTPS from OT Network Segment KQL

DETECTION ONLY

```
// OT devices should not be making DNS-over-HTTPS queries
// IOCONTROL uses DoH for C2 infrastructure resolution
CommonSecurityLog
| where DestinationPort == 443
| where DestinationIP in ("8.8.8.8","8.8.4.4","1.1.1.1","1.0.0.1","9.9.9.9")
| where SourceIP startswith "10.100."  // OT VLAN
| project TimeGenerated, SourceIP, DestinationIP, BytesSent, BytesReceived
```

Rule 3: Telegram C2 from OT/IoT

Telegram API Traffic from OT Segment KQL

DETECTION ONLY

```
// IoT/OT devices should not contact Telegram
// IOCONTROL uses Telegram bot API for C2
CommonSecurityLog
| where RequestURL has "api.telegram.org"
    or DestinationHostName has "telegram.org"
| where SourceIP startswith "10.100."  // OT VLAN
| project TimeGenerated, SourceIP, DestinationIP,
    RequestURL, BytesSent
```

Rule 4: MQTT from Non-Baselined Devices

Unexpected MQTT Traffic from OT Segment KQL

DETECTION ONLY

```
// Detect MQTT connections from devices not baselined for MQTT
// Requires a watchlist of known MQTT-using device IPs
let Baselined_MQTT_Devices = dynamic([
    // Add IPs of devices that legitimately use MQTT
    // "10.100.1.50", "10.100.1.51"
]);
CommonSecurityLog
| where DestinationPort in (8883, 1883)
| where SourceIP startswith "10.100."  // OT VLAN
| where not(SourceIP in (Baselined_MQTT_Devices))
| project TimeGenerated, SourceIP, DestinationIP,
    DestinationPort, BytesSent
```

C Appendix C: References

Government Advisories

[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

[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] **Dragos** - BAUXITE activity group tracking

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

Incident Reporting & Analysis

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

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

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

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

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

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

NEED HELP IMPLEMENTING THESE DETECTIONS?

Our threat hunting team can deploy, tune, and operationalize these detection rules in your environment.

- ✓ Detection rule deployment and tuning
- ✓ Managed threat hunting operations
- ✓ Incident response retainer

Contact Our Team

or

Automate continuous detection with BRACE, our sector-specific threat intelligence platform. See BRACE plans →