INTRUVENT

COMPREHENSIVE THREAT HUNTING GUIDE

CyberAv3ngers: OT/ICS Threat Hunt

Detecting IOControl malware, internet-exposed PLCs, default credential exploitation, and IRGC-CEC targeting of water, fuel, and dam infrastructure

Version 1.0
Classification TLP:CLEAR
Published March 17, 2026
Total Hunt Time 5.5 Hours
Threat Actor CyberAv3ngers / BAUXITE (IRGC-CEC)
Target Sectors Water/Wastewater, Fuel Management, Energy, Dams

Intruvent Technologies
INT-THG-2026-CYBERAV3NGERS-OT-v1.0

Table of Contents

Overview

Executive Summary 3
MITRE ATT&CK Mapping 4

Hunt Modules

Module 1: Internet-Exposed ICS Discovery 5
Module 2: Default Credential Audit 6
Module 3: IOControl Binary Hunt 7
Module 4: Anomalous MQTT Traffic Detection 8
Module 5: DNS-over-HTTPS from OT Devices 9
Module 6: PLC Ladder Logic Integrity 10
Module 7: Fuel Management System Audit 11
Module 8: IP Camera and Router Compromise 12
Module 9: Network Segmentation Validation 13
Module 10: C2 Infrastructure Detection 14

Appendices

Appendix A: Indicators of Compromise 15
Appendix B: Detection Rules 16
Appendix C: References 19

1 Executive Summary

AT A GLANCE

THREAT ACTOR CyberAv3ngers / BAUXITE (IRGC-CEC, Iran)	PRIMARY OBJECTIVE ICS/OT disruption via internet-exposed devices
ACTIVE SINCE 2020 (confirmed US targeting since Nov 2023)	TARGET SECTORS Water/Wastewater, Fuel Management, Energy, Dams
KEY DIFFERENTIATOR OT-first targeting; bypasses IT networks entirely	CUSTOM MALWARE IOControl (Linux backdoor for IoT/OT devices)

CyberAv3ngers (also tracked as BAUXITE by Dragos, MITRE G1027) is an IRGC Cyber-Electronic Command unit that directly attacks industrial control systems. Unlike most threat actors who pivot through IT environments to reach OT networks, CyberAv3ngers scans the internet for exposed PLCs, HMIs, fuel management systems, IP cameras, and routers, then exploits default credentials or known vulnerabilities to gain direct device access.

The group's Unitronics PLC defacement campaign (October 2023 to January 2024) compromised 75+ devices globally, including 34+ US water and wastewater facilities. The November 2023 compromise of the Aliquippa, Pennsylvania water authority was the first confirmed Iranian cyberattack on US water infrastructure. In December 2024, Claroty Team82 disclosed IOControl, a custom Linux backdoor deployed by CyberAv3ngers on IoT/OT devices using MQTT-based C2 and DNS-over-HTTPS for domain resolution.

This guide provides **10 hunt modules** designed for OT/ICS environments: discovering internet-exposed devices, auditing default credentials, hunting for IOControl artifacts, detecting anomalous MQTT and DoH traffic from OT segments, validating PLC program integrity, and identifying C2 communications. Total estimated hunt time is **5.5 hours**.

Threat Overview

CyberAv3ngers represents a distinct category of Iranian cyber threat. Where groups like APT33 and APT34 focus on espionage through IT network intrusion, CyberAv3ngers targets the physical process layer directly. The group exploits a fundamental gap in critical infrastructure security: OT devices connected to the internet with default credentials and no security monitoring.

The IOControl malware (disclosed by Claroty Team82, December 2024) elevated the group from opportunistic defacement to persistent access. IOControl runs on embedded Linux across multiple device architectures (ARM, MIPS, x86), uses MQTT over TLS for C2, resolves domains via DNS-over-HTTPS through Cloudflare, and employs modified UPX packing (magic bytes "ABC!" instead of "UPX!") to evade automated analysis. This malware has been recovered from Unitronics PLCs, Gasboy fuel management systems, Hikvision cameras, and D-Link routers.

The US Treasury sanctioned six IRGC-CEC officials on February 2, 2024, and the Rewards for Justice program offered $10 million for information. CISA issued Advisory AA23-335A. Despite these actions, the group remains active, with IOControl deployment on IP cameras and routers continuing into 2025-2026.

KEY CHARACTERISTICS

- IRGC-CEC state-sponsored (Iran)
- OT-first attack approach
- Default credential exploitation
- IOControl Linux backdoor
- MQTT C2 on port 8883 (TLS)
- DNS-over-HTTPS from OT devices
- Modified UPX packing ("ABC!")
- Unitronics Vision PLC targeting
- Gasboy/Orpak fuel system targeting
- OFAC-sanctioned (Feb 2024)

2 MITRE ATT&CK Mapping

The following techniques are sourced from MITRE ATT&CK G1027, CISA AA23-335A, and Claroty Team82 analysis. CyberAv3ngers operates across both the ICS and Enterprise ATT&CK matrices.

`T0812` ICS
Default Credentials
Primary initial access: Unitronics PLCs with default password "1111" (CVE-2023-6448)

`T0883` ICS
Internet Accessible Device
Targets PLCs, HMIs, and fuel systems directly exposed to the internet on known ports

`T0814` ICS
Denial of Service
Disruption of PLC operations and HMI availability at water treatment facilities

`T0826` ICS
Loss of Availability
PLCs taken offline; operators forced to manual control at Aliquippa water authority

`T0828` ICS
Loss of Productivity and Revenue
Fuel management system disruption; ~200 gas stations claimed affected

`T0829` ICS
Loss of View
HMI screens defaced with propaganda; operators lose visibility into process state

`T1078.001`
Default Accounts
Enterprise equivalent of T0812; exploitation of factory-default credentials on network devices

`T1110`
Brute Force
Credential brute-forcing against exposed device management interfaces

`T1071.001` NOVEL
Application Layer Protocol (MQTT)
IOControl uses MQTT over TLS (port 8883) for C2; first documented Iranian use of MQTT C2

`T1027.002` NOVEL
Software Packing
Modified UPX packing with "ABC!" magic bytes to evade standard unpacking tools

`T1547`
Boot or Logon Autostart Execution
IOControl persistence via init script at /etc/rc3.d/S93InitSystemd.sh

`T1082`
System Information Discovery
IOControl collects device type, OS version, and hardware details for C2 registration

`T1046`
Network Service Discovery
Port scanning from compromised OT devices to map internal network topology

`T1491.001`
Internal Defacement
HMI screens replaced with anti-Israel propaganda; signature CyberAv3ngers tactic

`T1565.001`
Stored Data Manipulation
Modification of PLC operational parameters and stored process data

`T1531`
Account Access Removal
Password changes on compromised devices to lock out legitimate administrators

3 Hunt Modules

1 Internet-Exposed ICS Discovery

Duration: 30 min Priority: CRITICAL

Objective: Identify any ICS/OT devices in your environment that are directly accessible from the internet, the primary attack surface CyberAv3ngers exploits.

Background

Every documented CyberAv3ngers intrusion began with an internet-exposed OT device. The group scans for Unitronics PLCs on TCP 20256 (PCOM protocol), Modbus devices on TCP 502, S7comm on TCP 102, and EtherNet/IP on TCP 44818. CISA AA23-335A specifically warned that Unitronics Vision PLCs are targeted because they use a well-known default password ("1111") and are frequently deployed with direct internet connectivity. This module determines whether your organization has the same exposure.

Hunt Procedure: External Port Scan for ICS Protocols

INVESTIGATION AID

BASH (NMAP)

```
# Scan your public IP ranges for common ICS/OT protocol ports
# CyberAv3ngers targets: TCP 20256 (Unitronics PCOM),
# TCP 502 (Modbus), TCP 102 (S7comm), TCP 44818 (EtherNet/IP)
# Run from OUTSIDE your network perimeter

nmap -sS -p 20256,502,102,44818,8883,1883 \
  --open -oA ics_exposure_scan \
  YOUR_PUBLIC_IP_RANGES

# Also check for Unitronics web interface (HTTP)
nmap -sS -p 80,443,8080 --script http-title \
  --open YOUR_PUBLIC_IP_RANGES | grep -i "unitronics\|vision"
```

Hunt Procedure: Firewall Log Analysis for Inbound ICS Traffic

DETECTION ONLY

KQL (AZURE SENTINEL / FIREWALL LOGS)

```
// Detect inbound connections to ICS protocol ports from external sources
// Any match indicates internet-exposed OT devices
CommonSecurityLog
| where TimeGenerated > ago(30d)
| where DestinationPort in (20256, 502, 102, 44818, 1883, 8883)
| where Direction == "Inbound" or NetworkDirection == "Inbound"
| where not(ipv4_is_private(SourceIP))
| summarize ConnectionCount=count(), DistinctSources=dcount(SourceIP)
    by DestinationIP, DestinationPort, bin(TimeGenerated, 1d)
| sort by ConnectionCount desc
```

☐ Run an external port scan against all public IP ranges for ICS protocol ports (20256, 502, 102, 44818)
☐ Review firewall logs for any permitted inbound traffic to these ports in the past 90 days
☐ Search Shodan/Censys for your organization's IP space with filters for Unitronics, Modbus, and S7comm
☐ Verify that all ICS devices are behind VPN or firewall with no direct internet access
☐ Document any exposed devices for immediate remediation

Any Internet-Exposed ICS Device Is an Active Risk

If this scan identifies any internet-exposed PLC, HMI, or SCADA device, treat it as an immediate finding. CyberAv3ngers actively scans the internet for these exact ports. Remove internet access to the device immediately and investigate for signs of prior compromise before restoring connectivity behind a VPN.

2 Default Credential Audit

Duration: 30 min Priority: CRITICAL

Objective: Verify that no PLC, HMI, IP camera, router, or fuel management system is using factory default credentials. CVE-2023-6448 (Unitronics default password "1111") enabled every known CyberAv3ngers PLC compromise.

Background

CVE-2023-6448 is a default password vulnerability in Unitronics Vision Series PLCs. The factory default password is "1111" and is well-documented in public Unitronics manuals. CyberAv3ngers exploited this credential across 75+ devices globally. CISA added CVE-2023-6448 to the Known Exploited Vulnerabilities catalog on December 11, 2023 (confirmed in Intruvent Golden CTI Database: actively exploited, CISA KEV). Beyond Unitronics, CyberAv3ngers also targets Hikvision cameras, D-Link routers, and Gasboy/Orpak systems, many of which ship with well-known default credentials.

Audit Procedure: Unitronics PLC Credentials

INVESTIGATION AID

MANUAL PROCEDURE

```
# Unitronics Vision PLC default credential check
# WARNING: Only perform on devices you are authorized to test

1. Connect to the PLC using VisiLogic software or web interface
2. Attempt authentication with default password: 1111
3. If authentication succeeds, the device is vulnerable to CVE-2023-6448
4. Change the password immediately to a unique, complex value
5. Document the device for your asset inventory

# Common default credentials to check across device types:
# Unitronics Vision: password "1111"
# Hikvision cameras: admin / 12345 (older models)
# D-Link routers: admin / admin (or blank password)
# Gasboy/Orpak: consult vendor documentation for defaults
```

Hunt Procedure: Authentication Attempts with Default Credentials

DETECTION ONLY

KQL (AZURE SENTINEL / SYSLOG)

```
// Detect authentication events on OT device management interfaces
// Look for successful logins that may indicate default credentials in use
Syslog
| where TimeGenerated > ago(30d)
| where SyslogMessage has_any ("login", "authentication", "auth")
| where SyslogMessage has_any ("unitronics", "hikvision", "dahua",
    "d-link", "gasboy", "orpak")
| project TimeGenerated, Computer, SyslogMessage, SourceIP
| sort by TimeGenerated desc
```

☐ Inventory all Unitronics Vision PLCs in your environment; test each for default password "1111"
☐ Audit credentials on all Hikvision cameras, Dahua cameras, and D-Link routers
☐ Verify Gasboy/Orpak fuel management system credentials are changed from defaults
☐ Implement a policy requiring unique, complex passwords for all OT/IoT devices
☐ Enable authentication logging on all devices that support it

CVE-2023-6448: CISA Known Exploited Vulnerability

This CVE is in the CISA Known Exploited Vulnerabilities catalog (added December 11, 2023) and is confirmed actively exploited by CyberAv3ngers. Federal agencies were required to remediate by December 2023. Any Unitronics PLC still using the default password "1111" should be considered at high risk of compromise.

3 IOControl Binary Hunt

Duration: 45 min Priority: HIGH

Objective: Search Linux-based IoT/OT devices for IOControl malware artifacts, including the binary, persistence scripts, and modified UPX headers.

Background

IOControl is a custom Linux backdoor deployed by CyberAv3ngers on embedded devices. Claroty Team82 (December 2024) documented the malware's installation at `/usr/bin/iocontrol` with a persistence init script at `/etc/rc3.d/S93InitSystemd.sh`. The binary uses modified UPX packing with "ABC!" magic bytes replacing the standard "UPX!" header. The working directory is `/tmp/iocontrol/`. IOControl has been recovered from Unitronics PLCs, Gasboy fuel systems, Hikvision cameras, and D-Link routers.

Hunt Procedure: IOControl File Artifacts

BLOCKING SAFE

BASH (LINUX / SSH TO OT DEVICES)

```
# Search for IOControl installation artifacts on Linux-based OT/IoT devices
# Source: Claroty Team82 (December 2024)
# Run via SSH on each accessible embedded Linux device

# Check for IOControl binary
ls -la /usr/bin/iocontrol 2>/dev/null

# Check for persistence script
ls -la /etc/rc3.d/S93InitSystemd.sh 2>/dev/null
cat /etc/rc3.d/S93InitSystemd.sh 2>/dev/null

# Check for working directory
ls -la /tmp/iocontrol/ 2>/dev/null

# Check for modified UPX magic bytes in any suspicious binaries
find /usr/bin /usr/sbin /tmp -type f -executable \
  -exec sh -c 'hexdump -C "$1" | head -5 | grep -q "ABC!" && echo "MODIFIED UPX: $1"' _ {} \;

# SHA256 hash check against known IOControl sample
sha256sum /usr/bin/iocontrol 2>/dev/null
# Expected match: 1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498
```

Hunt Procedure: IOControl Process Detection

BLOCKING SAFE

BASH (LINUX / SSH TO OT DEVICES)

```
# Check for running IOControl process
ps aux | grep -i iocontrol | grep -v grep

# Check for processes with MQTT connections (port 8883)
netstat -tlnp 2>/dev/null | grep 8883
ss -tlnp 2>/dev/null | grep 8883

# Check for suspicious outbound connections
netstat -anp 2>/dev/null | grep -E "(159\.100\.6\.69|8883)"
ss -anp 2>/dev/null | grep -E "(159\.100\.6\.69|8883)"

# Check init scripts for persistence
ls -la /etc/rc*.d/ | grep -i "init\|systemd\|iocontrol"
```

Hunt Procedure: Endpoint Detection (If EDR Covers OT Devices)

BLOCKING SAFE

KQL (MICROSOFT DEFENDER FOR ENDPOINT / LINUX AGENTS)

```
// Search for IOControl file indicators on managed Linux endpoints
// Source: Claroty Team82 (December 2024)
let IOControlHash = "1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498";
DeviceFileEvents
| where SHA256 == IOControlHash
    or FileName == "iocontrol"
    or FolderPath has "/usr/bin/iocontrol"
    or FolderPath has "/tmp/iocontrol"
    or FileName == "S93InitSystemd.sh"
| project Timestamp, DeviceName, FileName, FolderPath, SHA256, ActionType
| sort by Timestamp desc
```

☐ SSH into each accessible Linux-based OT/IoT device and check for IOControl file paths
☐ Verify SHA256 hash of any file at /usr/bin/iocontrol against the known IOControl hash
☐ Search for the persistence script S93InitSystemd.sh in init directories
☐ Check for binaries with modified UPX headers ("ABC!" magic bytes)
☐ If IOControl is found, isolate the device immediately and preserve forensic evidence

Any IOControl Match Is Confirmed Compromise

The IOControl binary, its persistence script, and its working directory are unique to CyberAv3ngers operations. Any match on file paths, hashes, or modified UPX headers confirms an active or previous CyberAv3ngers intrusion. Isolate the device, preserve the filesystem image, and escalate to incident response immediately.

4 Anomalous MQTT Traffic Detection

Duration: 30 min Priority: HIGH

Objective: Detect MQTT traffic on port 8883 (TLS) originating from OT network segments where MQTT is not expected, a signature IOControl C2 indicator.

Background

IOControl uses MQTT (Message Queuing Telemetry Transport) over TLS on port 8883 as its primary C2 channel (Claroty Team82, December 2024). MQTT is a lightweight publish/subscribe protocol designed for IoT devices. While MQTT is legitimate in some IoT deployments, its presence on OT network segments (where PLCs, HMIs, and SCADA systems operate) is unusual. CyberAv3ngers chose MQTT because it blends with legitimate IoT traffic and is rarely monitored by security tools. Port 1883 (unencrypted MQTT) may also be used in some variants.

Hunt Procedure: MQTT Traffic from OT Segments

DETECTION ONLY

KQL (AZURE SENTINEL / FIREWALL LOGS)

```
// Detect MQTT traffic (ports 1883, 8883) from OT network segments
// Customize OT_SUBNET to match your OT network addressing
let OT_Subnets = dynamic(["10.10.0.0/16", "172.16.100.0/24"]);
// Replace with your actual OT network ranges
CommonSecurityLog
| where TimeGenerated > ago(30d)
| where DestinationPort in (1883, 8883)
| where ipv4_is_in_any_range(SourceIP, OT_Subnets)
| summarize ConnectionCount=count(),
    DistinctDestinations=dcount(DestinationIP),
    Destinations=make_set(DestinationIP)
    by SourceIP, DestinationPort, bin(TimeGenerated, 1d)
| sort by ConnectionCount desc
```

Hunt Procedure: Network Capture for MQTT Identification

INVESTIGATION AID

BASH (TCPDUMP / NETWORK TAP)

```
# Capture MQTT traffic on OT network segments
# Run on a network TAP or SPAN port monitoring OT traffic
# WARNING: Ensure packet capture is authorized and does not impact OT operations

# Capture traffic to MQTT ports
tcpdump -i eth0 -w mqtt_hunt.pcap \
  'port 8883 or port 1883' -c 10000

# Analyze in Wireshark with MQTT dissector
# Filter: mqtt || tls.handshake.extensions_server_name contains "mqtt"
```

☐ Review firewall and flow logs for any MQTT traffic (ports 1883, 8883) from OT network segments
☐ Determine if any legitimate MQTT brokers exist in your OT environment; document them as baselines
☐ Investigate any MQTT traffic to external (internet) destinations from OT devices
☐ If MQTT traffic is detected from devices that should not use it, investigate the source device for IOControl

MQTT May Be Legitimate in Some Environments

Some industrial IoT platforms (SCADA gateways, building management systems, smart sensors) use MQTT for telemetry. The key indicator is unexpected MQTT traffic: from devices that do not normally use MQTT, to external destinations, or from traditional OT equipment (PLCs, HMIs) that should not make MQTT connections. Baseline your environment before classifying MQTT traffic as malicious.

5 DNS-over-HTTPS from OT Devices

Duration: 30 min Priority: HIGH

Objective: Detect DNS-over-HTTPS (DoH) traffic to Cloudflare's 1.1.1.1 resolver originating from OT devices that should never generate DoH queries.

Background

IOControl resolves C2 domain names using DNS-over-HTTPS through Cloudflare's 1.1.1.1 resolver (Claroty Team82, December 2024). This technique bypasses traditional DNS monitoring because the queries are encrypted within HTTPS traffic. PLCs, HMIs, IP cameras, and fuel management systems do not make DoH requests under normal operations. Any DoH traffic from an OT device is a high-fidelity anomaly.

Hunt Procedure: DoH Traffic to Cloudflare from OT Segments

DETECTION ONLY

KQL (AZURE SENTINEL / FIREWALL LOGS)

```
// Detect HTTPS connections to Cloudflare DoH resolver from OT network segments
// IOControl uses 1.1.1.1 for DNS-over-HTTPS (Claroty Team82, Dec 2024)
let CloudflareDoH = dynamic(["1.1.1.1", "1.0.0.1",
    "2606:4700:4700::1111", "2606:4700:4700::1001"]);
let OT_Subnets = dynamic(["10.10.0.0/16", "172.16.100.0/24"]);
CommonSecurityLog
| where TimeGenerated > ago(30d)
| where DestinationPort == 443
| where DestinationIP in (CloudflareDoH)
| where ipv4_is_in_any_range(SourceIP, OT_Subnets)
| summarize ConnectionCount=count()
    by SourceIP, DestinationIP, bin(TimeGenerated, 1h)
| sort by ConnectionCount desc
```

Hunt Procedure: TLS SNI Analysis for DoH Domains

INVESTIGATION AID

BASH (ZEEK / NETWORK MONITOR)

```
# If Zeek is deployed on OT network monitoring, search for DoH indicators
# Look for TLS connections to cloudflare-dns.com from OT devices

grep -i "cloudflare-dns.com\|1dot1dot1dot1.cloudflare-dns.com" \
  /path/to/zeek/logs/ssl.log

# Also check for connections to known DoH endpoint paths
grep -i "/dns-query" /path/to/zeek/logs/http.log
```

☐ Search firewall logs for HTTPS (port 443) connections from OT devices to 1.1.1.1 or 1.0.0.1
☐ Review proxy logs for DoH endpoint URLs (cloudflare-dns.com/dns-query)
☐ If Zeek or similar NSM is deployed on OT segments, search TLS logs for Cloudflare DoH SNI values
☐ Investigate any OT device making HTTPS connections to 1.1.1.1 for IOControl compromise

High-Fidelity Indicator for OT Environments

DoH traffic from a PLC, HMI, IP camera, or fuel management controller is almost certainly anomalous. These devices use standard DNS (port 53) if they make DNS queries at all. DoH traffic from an OT device strongly suggests the presence of IOControl or similar malware. Do not block 1.1.1.1 globally (legitimate users rely on it), but alert on and investigate any OT device making such connections.

6 PLC Ladder Logic Integrity

Duration: 45 min Priority: HIGH

Objective: Verify that PLC programs and HMI configurations have not been modified by CyberAv3ngers. The group has defaced HMI screens and, in more advanced operations, modified PLC operational parameters.

Background

CyberAv3ngers' initial campaigns focused on HMI defacement: replacing the operator display with anti-Israel propaganda (MITRE T0829, Loss of View). However, the group also modifies PLC operational parameters (T1565.001, Stored Data Manipulation) and can remove administrator access (T1531, Account Access Removal). The deployment of IOControl on PLCs enables persistent access that could be used for more destructive manipulation of physical processes. Organizations should verify PLC program integrity against known-good baselines.

Audit Procedure: PLC Program Comparison

INVESTIGATION AID

MANUAL PROCEDURE

```
# PLC Ladder Logic Integrity Verification
# Perform during a maintenance window or with process engineer oversight

1. Retrieve the current PLC program using vendor software:
   - Unitronics: VisiLogic (Upload from PLC)
   - Other vendors: use the appropriate engineering workstation

2. Compare the uploaded program against the known-good baseline:
   - Binary comparison (hash the program files)
   - Logic comparison (visual diff in engineering software)
   - Pay attention to: timer values, setpoints, alarm limits

3. Check HMI screens for unauthorized modifications:
   - Verify all display pages show expected content
   - Check for hidden pages or modified navigation

4. Review PLC user accounts:
   - Verify no unauthorized accounts have been added
   - Confirm administrator passwords have not been changed
   - Check for account lockouts that may indicate brute-force attempts

5. Verify PLC firmware version matches expected version:
   - Compare against vendor-published firmware versions
   - Check for unauthorized firmware modifications
```

☐ Upload current PLC programs and compare against known-good baselines (hash comparison)
☐ Verify HMI display pages show expected content (no defacement)
☐ Audit PLC user accounts for unauthorized additions or password changes
☐ Confirm PLC firmware versions match expected values
☐ Check operational parameters (setpoints, timer values, alarm limits) against engineering specifications

Coordinate with Process Engineers

PLC program verification must be performed in coordination with process engineers who understand the expected logic. Uploading or comparing programs on live PLCs carries operational risk. Schedule this activity during a maintenance window or ensure a qualified engineer is present to validate that the comparison process will not disrupt operations.

7 Fuel Management System Audit

Duration: 30 min Priority: MEDIUM

Objective: Check Gasboy and Orpak fuel management systems for IOControl indicators and unauthorized access. CyberAv3ngers targeted these systems in a two-wave campaign from October 2023 through August 2024.

Background

CyberAv3ngers targeted Orpak fuel management systems in Israeli gas stations (October 2023) and Gasboy fuel management systems in the United States (2024). Claroty Team82 confirmed IOControl malware samples were recovered from Gasboy fuel management devices in the US. These systems manage fuel dispensing, tank level monitoring, and transaction processing. Compromise could enable fuel theft, data manipulation, or operational disruption.

Audit Procedure: Gasboy/Orpak Device Check

INVESTIGATION AID

MANUAL / SSH PROCEDURE

```
# Fuel management system IOControl indicator check
# Applicable to Gasboy and Orpak systems running embedded Linux

# 1. Check for IOControl artifacts (same as Module 3)
ls -la /usr/bin/iocontrol 2>/dev/null
ls -la /etc/rc3.d/S93InitSystemd.sh 2>/dev/null
ls -la /tmp/iocontrol/ 2>/dev/null

# 2. Check for unexpected network connections
netstat -anp 2>/dev/null | grep -E "(8883|159\.100\.6\.69)"

# 3. Verify system integrity
# Compare running processes against known-good baseline
ps aux > /tmp/current_processes.txt
# Diff against baseline process list

# 4. Check for unauthorized user accounts
cat /etc/passwd | grep -v "nologin\|false"

# 5. Verify fuel transaction data integrity
# Compare physical tank levels against reported digital values
# Discrepancies may indicate data manipulation
```

☐ Identify all Gasboy and Orpak systems in your environment
☐ Check each system for IOControl file artifacts and network indicators
☐ Verify fuel transaction data integrity (physical vs. reported levels)
☐ Audit user accounts and access logs on fuel management controllers
☐ Verify these systems are not directly accessible from the internet

8 IP Camera and Router Compromise

Duration: 30 min Priority: MEDIUM

Objective: Hunt for IOControl malware on Hikvision cameras, Dahua cameras, and D-Link routers. CyberAv3ngers uses these devices as entry points into OT networks and as relay infrastructure.

Background

Claroty Team82 (December 2024) documented IOControl deployment on Hikvision IP cameras, Dahua IP cameras, and D-Link routers. These devices are frequently deployed in and around OT environments for physical security monitoring. They run embedded Linux and are often left with default credentials or unpatched firmware. Once compromised, they can serve as pivot points into segmented OT networks or as relay nodes for C2 traffic.

Hunt Procedure: Camera and Router IOControl Check

INVESTIGATION AID

BASH (SSH WHERE AVAILABLE)

```
# Check IP cameras and routers for IOControl indicators
# NOTE: Not all devices support SSH access; use device management
# interfaces or firmware extraction where SSH is unavailable

# For devices with SSH access:
ls -la /usr/bin/iocontrol 2>/dev/null
ls -la /etc/rc3.d/S93InitSystemd.sh 2>/dev/null
netstat -anp 2>/dev/null | grep -E "(8883|1883)"
ps aux | grep -v grep | grep -i "iocontrol\|mqtt"

# For devices without SSH, check from the network:
# Look for MQTT traffic (8883) from camera/router IP addresses
# Look for DoH traffic (443 to 1.1.1.1) from camera/router IPs
```

☐ Inventory all Hikvision, Dahua, and D-Link devices in your environment
☐ Verify firmware is updated to the latest vendor-supported version
☐ Confirm default credentials have been changed on all devices
☐ Check network logs for MQTT or DoH traffic originating from camera/router IPs
☐ Where possible, SSH into devices and check for IOControl file artifacts

9 Network Segmentation Validation

Duration: 30 min Priority: MEDIUM

Objective: Verify that OT/IT network boundaries are enforced and that no unauthorized cross-segment traffic could enable CyberAv3ngers to pivot from compromised IoT devices into critical OT systems.

Background

CyberAv3ngers compromises IP cameras and routers that often sit at the boundary between IT and OT networks. If network segmentation is weak or misconfigured, a compromised camera could provide a path from the internet into OT network segments containing PLCs and SCADA systems. IOControl includes port scanning capability (T1046), which CyberAv3ngers can use to map internal networks from a compromised boundary device.

Hunt Procedure: Cross-Segment Traffic Analysis

DETECTION ONLY

KQL (AZURE SENTINEL / FIREWALL LOGS)

```
// Detect traffic crossing OT/IT network boundaries
// Customize subnets to match your network architecture
let OT_Subnets = dynamic(["10.10.0.0/16", "172.16.100.0/24"]);
let IT_Subnets = dynamic(["10.0.0.0/16", "172.16.0.0/24"]);
CommonSecurityLog
| where TimeGenerated > ago(7d)
| where (ipv4_is_in_any_range(SourceIP, OT_Subnets)
    and ipv4_is_in_any_range(DestinationIP, IT_Subnets))
    or (ipv4_is_in_any_range(SourceIP, IT_Subnets)
    and ipv4_is_in_any_range(DestinationIP, OT_Subnets))
| summarize ConnectionCount=count(),
    DistinctPorts=dcount(DestinationPort),
    Ports=make_set(DestinationPort)
    by SourceIP, DestinationIP, bin(TimeGenerated, 1h)
| where ConnectionCount > 50 or DistinctPorts > 5
| sort by ConnectionCount desc
```

Hunt Procedure: Port Scanning from OT Devices

DETECTION ONLY

KQL (AZURE SENTINEL / FIREWALL LOGS)

```
// Detect port scanning behavior from OT network devices
// IOControl includes port scanning capability (Claroty Team82)
let OT_Subnets = dynamic(["10.10.0.0/16", "172.16.100.0/24"]);
CommonSecurityLog
| where TimeGenerated > ago(7d)
| where ipv4_is_in_any_range(SourceIP, OT_Subnets)
| summarize DistinctPorts=dcount(DestinationPort),
    DistinctDests=dcount(DestinationIP),
    Ports=make_set(DestinationPort, 20)
    by SourceIP, bin(TimeGenerated, 10m)
| where DistinctPorts > 20 or DistinctDests > 10
| sort by DistinctPorts desc
```

☐ Review firewall rules controlling traffic between IT and OT network segments
☐ Verify that OT devices cannot initiate connections to the internet directly
☐ Search for port scanning activity originating from OT device IP addresses
☐ Confirm that IP cameras and routers on OT segments cannot route traffic to IT networks
☐ Document any segmentation gaps for remediation

10 C2 Infrastructure Detection

Duration: 30 min Priority: MEDIUM

Objective: Hunt for network connections to known CyberAv3ngers C2 infrastructure and detect anomalous outbound traffic from OT network segments.

Background

IOControl communicates with C2 infrastructure via MQTT over TLS. Known C2 indicators include IP address 159.100.6.69 and domains uuokhhfsdlk.tylarion867mino.com and ocferda.com (Claroty Team82, December 2024). Because IOControl uses DNS-over-HTTPS for domain resolution, standard DNS logs will not capture these queries. Network flow data, firewall logs, and proxy logs are the primary detection sources for C2 traffic.

Hunt Procedure: Known C2 IP and Domain Detection

BLOCKING SAFE

KQL (AZURE SENTINEL / FIREWALL + DNS)

```
// Search for connections to known CyberAv3ngers C2 infrastructure
// Source: Claroty Team82 (December 2024)
let C2_IPs = dynamic(["159.100.6.69"]);
let C2_Domains = dynamic([
    "uuokhhfsdlk.tylarion867mino.com",
    "ocferda.com",
    "tylarion867mino.com"
]);

// Network connections to C2 IPs
CommonSecurityLog
| where TimeGenerated > ago(90d)
| where DestinationIP in (C2_IPs) or SourceIP in (C2_IPs)
| project TimeGenerated, SourceIP, DestinationIP, DestinationPort,
    Protocol, DeviceAction
| sort by TimeGenerated desc;

// DNS lookups for C2 domains (will only work if DoH is not used)
DnsEvents
| where TimeGenerated > ago(90d)
| where Name has_any (C2_Domains)
| project TimeGenerated, ClientIP, Name, IPAddresses, QueryType
| sort by TimeGenerated desc
```

Hunt Procedure: Anomalous Outbound from OT Segments

DETECTION ONLY

KQL (AZURE SENTINEL / FIREWALL LOGS)

```
// Detect any outbound internet connections from OT network segments
// OT devices should not initiate internet connections
let OT_Subnets = dynamic(["10.10.0.0/16", "172.16.100.0/24"]);
CommonSecurityLog
| where TimeGenerated > ago(30d)
| where ipv4_is_in_any_range(SourceIP, OT_Subnets)
| where not(ipv4_is_private(DestinationIP))
| summarize ConnectionCount=count(),
    DistinctDests=dcount(DestinationIP),
    Destinations=make_set(DestinationIP, 20),
    Ports=make_set(DestinationPort, 10)
    by SourceIP, bin(TimeGenerated, 1d)
| sort by ConnectionCount desc
```

☐ Search all network logs for connections to 159.100.6.69 in the past 90 days
☐ Search DNS logs for lookups of tylarion867mino.com, ocferda.com, and subdomains
☐ Review all outbound internet connections from OT network segments; each should have a documented business justification
☐ If C2 indicators are found, isolate affected devices and initiate incident response

DNS-over-HTTPS Limits DNS Log Visibility

IOControl uses DNS-over-HTTPS (Cloudflare 1.1.1.1) to resolve C2 domains. Standard DNS logs will not capture these lookups. Detection relies on network flow data showing connections to C2 IPs, or on identifying DoH traffic from OT devices (see Module 5). If your environment uses TLS inspection on OT egress traffic, DoH queries may be visible in proxy logs.

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 init script	Claroty Team82 (Dec 2024)
Directory	`/tmp/iocontrol/`	IOControl working directory	Claroty Team82 (Dec 2024)
UPX Magic	`ABC!` (replaces `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	CISA AA23-335A
Port	TCP 502	Modbus (targeted protocol)	CISA AA23-335A

IOC Blocking Guidance

Tier 1: Block (High Confidence)
SHA256 hash, IOControl file paths, C2 domains (uuokhhfsdlk.tylarion867mino.com, ocferda.com): Confirmed CyberAv3ngers infrastructure. No legitimate use. Safe to block at DNS sinkhole, firewall, and endpoint detection layers.

Tier 2: Alert/Monitor (Shared Infrastructure)
IP 159.100.6.69: Verify hosting provider before network-level block. Alert and require analyst review. **Port 8883 (MQTT TLS):** Legitimate IoT protocol. Do not block globally. Alert on unexpected MQTT from OT segments only. **Cloudflare 1.1.1.1:** Used by millions of legitimate users. Do not block. Alert on DoH from OT devices only.

Tier 3: Investigate (Contextual)
Ports 20256, 502, 102, 44818: Legitimate ICS protocol ports. Do not block. Restrict to authorized management stations. Investigate external connections. **Default credential "1111":** Not a network indicator. Remediate through password change policy.

B Appendix B: Detection Rules

KQL Detection Rules

Detection Rule Deployment Guidance

All detection rules include safety labels indicating their appropriate deployment scope. Rules labeled BLOCKING SAFE target specific, confirmed-malicious indicators. Rules labeled DETECTION ONLY target broader patterns and require analyst review before action. Adapt OT subnet ranges and device lists to match your environment before deployment.

IOControl File Indicators on Linux Endpoints

KQL

BLOCKING SAFE

```
// Detect IOControl malware artifacts on managed Linux endpoints
// Source: Claroty Team82 (December 2024)
let IOControlHash = "1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498";
DeviceFileEvents
| where SHA256 == IOControlHash
    or FileName == "iocontrol"
    or FolderPath has "/usr/bin/iocontrol"
    or FolderPath has "/tmp/iocontrol"
    or FileName == "S93InitSystemd.sh"
| project Timestamp, DeviceName, FileName, FolderPath, SHA256, ActionType
```

MQTT Traffic from OT Network Segments

KQL

DETECTION ONLY

```
// Detect MQTT traffic from OT segments (IOControl C2 indicator)
// Customize OT_Subnets for your environment
let OT_Subnets = dynamic(["10.10.0.0/16", "172.16.100.0/24"]);
CommonSecurityLog
| where DestinationPort in (1883, 8883)
| where ipv4_is_in_any_range(SourceIP, OT_Subnets)
| summarize Connections=count(), Destinations=make_set(DestinationIP)
    by SourceIP, DestinationPort, bin(TimeGenerated, 1h)
| sort by Connections desc
```

DNS-over-HTTPS from OT Devices

KQL

DETECTION ONLY

```
// Detect HTTPS to Cloudflare DoH from OT network segments
// IOControl uses DoH via 1.1.1.1 (Claroty Team82, Dec 2024)
let CloudflareDoH = dynamic(["1.1.1.1", "1.0.0.1"]);
let OT_Subnets = dynamic(["10.10.0.0/16", "172.16.100.0/24"]);
CommonSecurityLog
| where DestinationPort == 443
| where DestinationIP in (CloudflareDoH)
| where ipv4_is_in_any_range(SourceIP, OT_Subnets)
| project TimeGenerated, SourceIP, DestinationIP, DeviceAction
```

Inbound Connections to ICS Protocol Ports

KQL

DETECTION ONLY

```
// Alert on inbound connections to ICS ports from external sources
// CyberAv3ngers scans for these ports (CISA AA23-335A)
CommonSecurityLog
| where DestinationPort in (20256, 502, 102, 44818)
| where not(ipv4_is_private(SourceIP))
| project TimeGenerated, SourceIP, DestinationIP, DestinationPort,
    DeviceAction, Protocol
| sort by TimeGenerated desc
```

Sigma Rules

IOControl Persistence Mechanism

SIGMA

BLOCKING SAFE

```
title: CyberAv3ngers IOControl Persistence Script Detection
id: ca3-iocontrol-persist-001
status: experimental
description: >
    Detects creation or modification of IOControl persistence
    init script used by CyberAv3ngers on Linux IoT/OT devices.
    Source: Claroty Team82 (December 2024)
references:
    - https://claroty.com/team82/research/iocontrol-cyberav3ngers-malware
author: Intruvent Technologies
date: 2026/03/17
tags:
    - attack.persistence
    - attack.t1547
logsource:
    product: linux
    category: file_event
detection:
    selection_path:
        TargetFilename|contains:
            - '/etc/rc3.d/S93InitSystemd.sh'
            - '/usr/bin/iocontrol'
            - '/tmp/iocontrol/'
    condition: selection_path
falsepositives:
    - None known. These file paths are specific to IOControl malware.
level: critical
```

Anomalous DoH from OT Devices

SIGMA

DETECTION ONLY

```
title: DNS-over-HTTPS from OT Network Devices
id: ca3-doh-ot-001
status: experimental
description: >
    Detects HTTPS connections to Cloudflare DoH resolver from
    OT network segments. IOControl uses DoH for C2 domain resolution.
    OT devices do not generate DoH traffic under normal operations.
    Source: Claroty Team82 (December 2024)
references:
    - https://claroty.com/team82/research/iocontrol-cyberav3ngers-malware
author: Intruvent Technologies
date: 2026/03/17
tags:
    - attack.command_and_control
    - attack.t1071.001
logsource:
    category: firewall
detection:
    selection:
        dst_ip:
            - '1.1.1.1'
            - '1.0.0.1'
        dst_port: 443
    filter_it_segments:
        src_ip|cidr:
            - '10.0.0.0/8'    # Customize: exclude IT subnets
    condition: selection and not filter_it_segments
falsepositives:
    - IoT devices that legitimately use DoH for connectivity checks.
    - Network management tools that use Cloudflare DNS.
level: high
```

YARA Rules

IOControl Modified UPX Binary Detection

YARA

BLOCKING SAFE

```
rule CyberAv3ngers_IOControl_Modified_UPX
{
    meta:
        description = "Detects IOControl malware with modified UPX packing"
        author = "Intruvent Technologies"
        date = "2026-03-17"
        reference = "Claroty Team82, December 2024"
        threat_actor = "CyberAv3ngers / BAUXITE / G1027"
        severity = "critical"
        tlp = "clear"

    strings:
        // Modified UPX magic bytes (replaces standard "UPX!")
        $upx_modified = "ABC!" ascii
        // Standard UPX section names still present
        $upx_section1 = "UPX0" ascii
        $upx_section2 = "UPX1" ascii
        // IOControl-specific strings
        $path1 = "/usr/bin/iocontrol" ascii
        $path2 = "/tmp/iocontrol" ascii
        $path3 = "S93InitSystemd" ascii
        // MQTT-related strings
        $mqtt1 = "8883" ascii
        $mqtt2 = "MQTT" ascii

    condition:
        uint32(0) == 0x464C457F  // ELF header
        and $upx_modified
        and (1 of ($upx_section*))
        and (1 of ($path*) or 2 of ($mqtt*))
}
```

IOControl Binary Hash Match

YARA

BLOCKING SAFE

```
rule CyberAv3ngers_IOControl_Hash
{
    meta:
        description = "Detects known IOControl binary by SHA256 hash"
        author = "Intruvent Technologies"
        date = "2026-03-17"
        reference = "Claroty Team82, December 2024"
        hash = "1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498"
        severity = "critical"

    condition:
        hash.sha256(0, filesize) ==
            "1b39f9b2b96a6586c4a11ab2fdbff8fdf16ba5a0ac7603149023d73f33b84498"
}

import "hash"
```

C Appendix C: 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: CISA KEV, actively exploited, Unitronics Vision PLC and HMI. CyberAv3ngers confirmed in sector targeting data for Water/Wastewater and Dams sectors.

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

[10] MITRE ATT&CK for ICS, Techniques: T0812 (Default Credentials), T0814 (Denial of Service), T0883 (Internet Accessible Device), T0826 (Loss of Availability), T0828 (Loss of Productivity and Revenue), T0829 (Loss of View).

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 →