New IOCONTROL malware used in critical infrastructure attacks

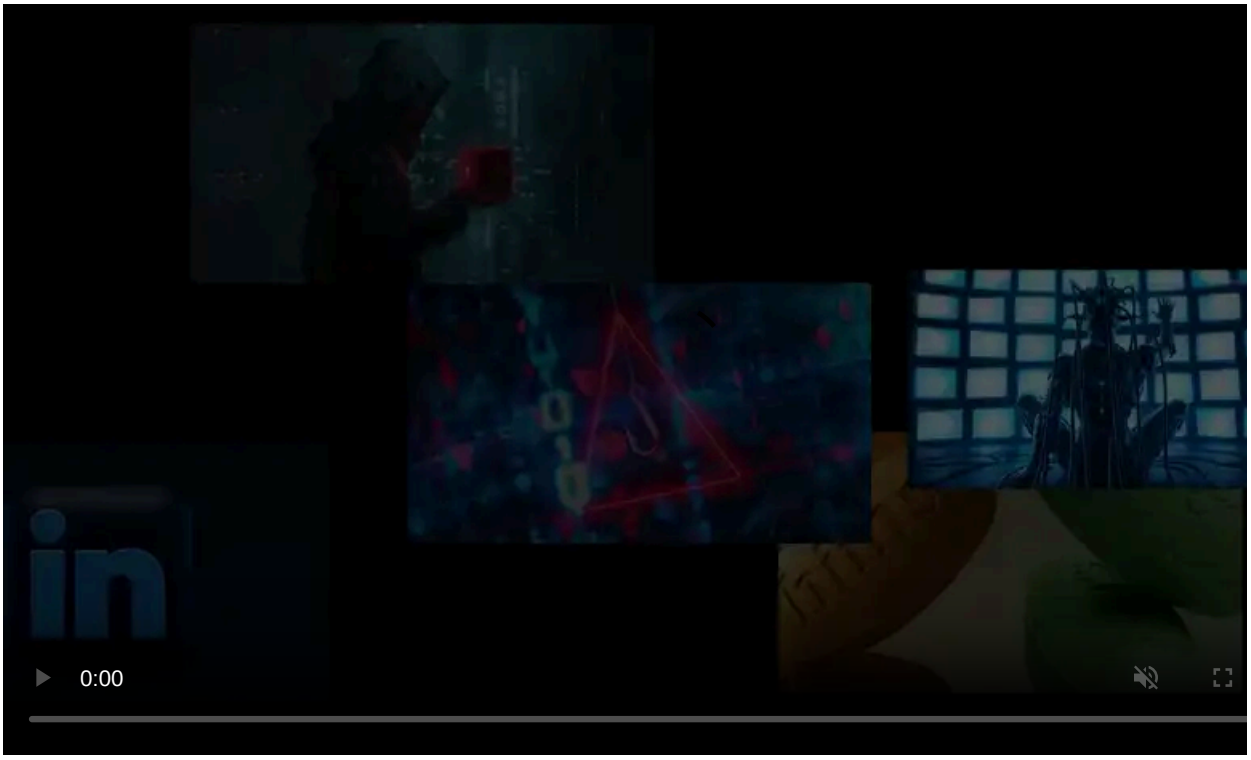
By Bill Toulas

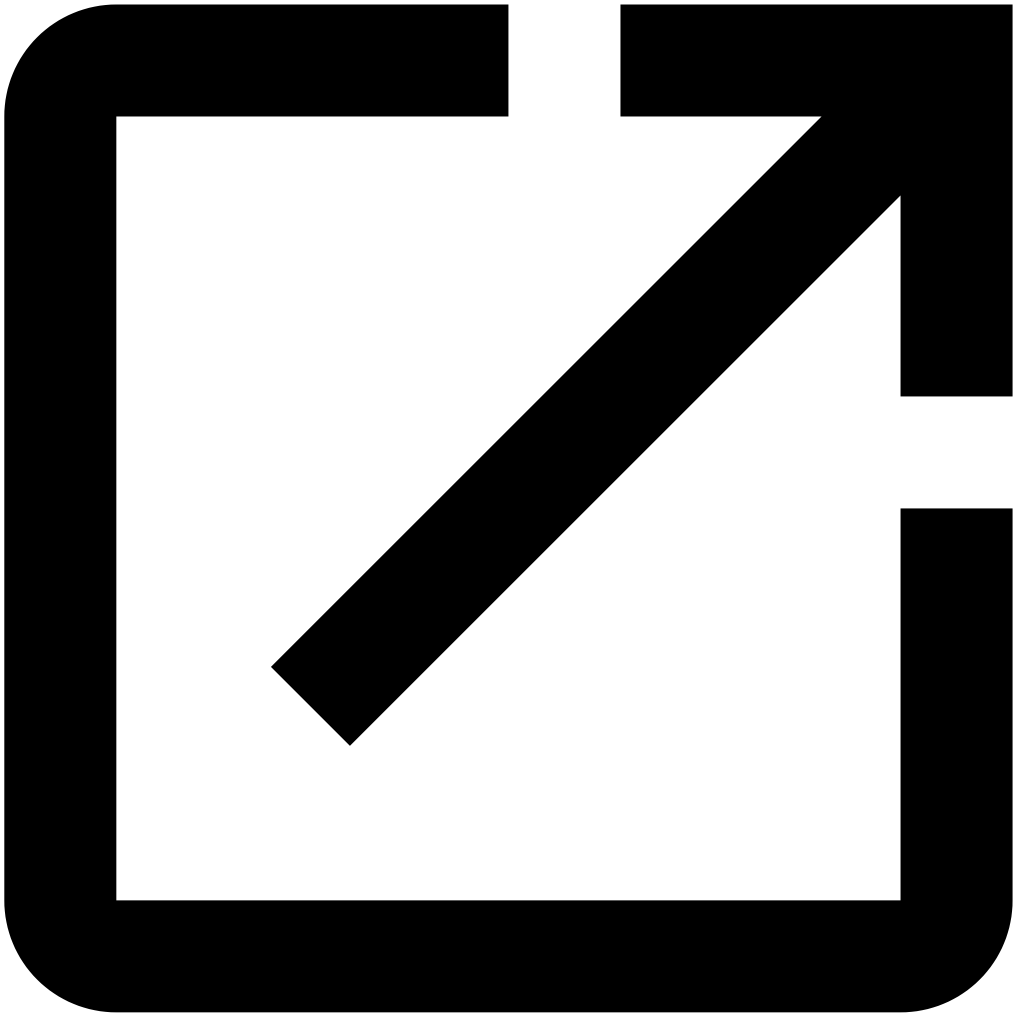
Published: 2024-12-12 · Archived: 2026-04-05 17:39:41 UTC

Iranian threat actors are utilizing a new malware named IOCONTROL to compromise Internet of Things (IoT) devices and OT/SCADA systems used by critical infrastructure in Israel and the United States.

Targeted devices include routers, programmable logic controllers (PLCs), human-machine interfaces (HMIs), IP cameras, firewalls, and fuel management systems.

The malware's modular nature makes it capable of compromising a broad spectrum of devices from various manufacturers, including D-Link, Hikvision, Baicells, Red Lion, Orpak, Phoenix Contact, Teltonika, and Unitronics.


0:00



Visit Advertiser websiteGO TO PAGE

Claroty's Team82 researchers, who have discovered and sampled IOCONTROL for analysis, report that it's a nation-state cyberweapon that can cause significant disruptions in critical infrastructure.

Given the ongoing geopolitical conflict, IOCONTROL is currently used to target Israel and U.S. systems, like Orpak and Gasboy fuel management systems.

The tool is reportedly linked to an Iranian hacking group known as CyberAv3ngers, who have shown interest in attacking industrial systems in the past. OpenAI also recently reported that the threat group uses ChatGPT to crack PLCs, develop custom bash and Python exploit scripts, and plan its post-compromise activity.

IOCONTROL attacks

Claroty extracted malware samples from a Gasboy fuel control system, specifically the device's payment terminal (OrPT), but the researchers do not know precisely how the hackers infected it with IOCONTROL.

Inside those devices, IOCONTROL could control pumps, payment terminals, and other peripheral systems, potentially causing disruption or data theft.

The threat actors have claimed to compromise 200 gas stations in Israel and the U.S. on Telegram, which aligns with Claroty's findings.

These attacks occurred in late 2023, around the same time as the defacement of Unitronics Vision PLC/HMI devices in water treatment facilities, but the researchers report that new campaigns emerged in mid-2024.

As of December 10, 2024, the UPX-packed malware binary is detected by none of the 66 VirusTotal antivirus engines.

Gasboy fuel control system from where the malware was extracted
Source: Claroty

Malware capabilities

The malware, which is stored in the '/usr/bin/' directory under the name 'iocontrol.' uses a modular configuration to adapt to different vendors and device types, targeting a broad spectrum of system architectures.

It uses a persistence script ('S93InitSystemd.sh') to execute the malware process ('iocontrol') upon system boot, so restarting the device does not deactivate it.

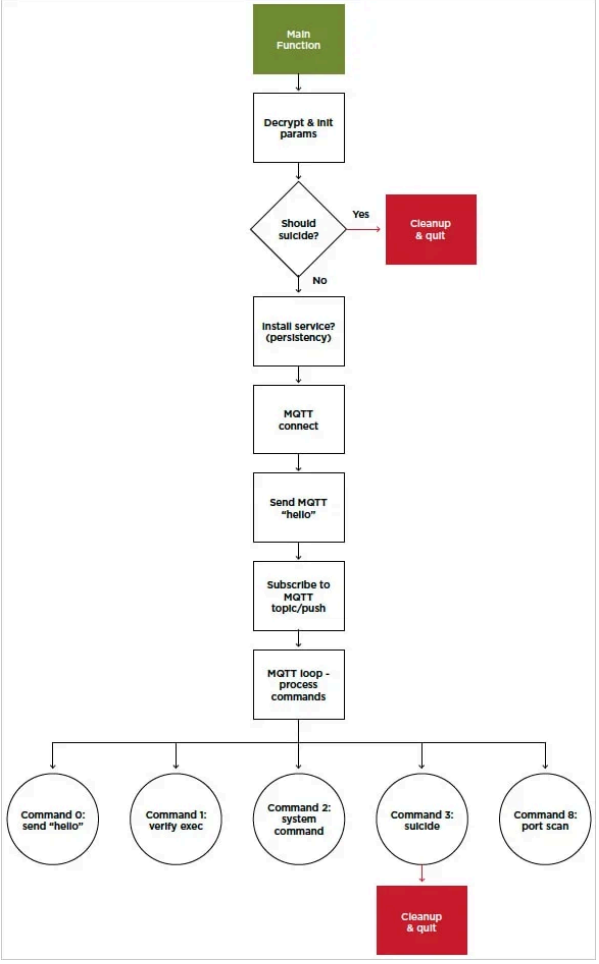
It uses the MQTT protocol through port 8883 to communicate with its command and control (C2) server, which is a standard channel and protocol for IoT devices. Unique device IDs are embedded into the MQTT credentials for better control.

DNS over HTTPS (DoH) is used to resolve the C2 domains while evading network traffic monitoring tools, and the malware's configuration is encrypted using AES-256-CBC.

The commands IOCONTROL supports are the following:

- **Send "hello"**: Reports detailed system information (e.g., hostname, current user, device model) to the C2.
- **Check exec**: Confirms the malware binary is properly installed and executable.
- **Execute command**: Runs arbitrary OS commands via system calls and reports output.
- **Self-delete**: Removes its own binaries, scripts, and logs to evade detection.
- **Port scan**: Scans specified IP ranges and ports to identify other potential targets.

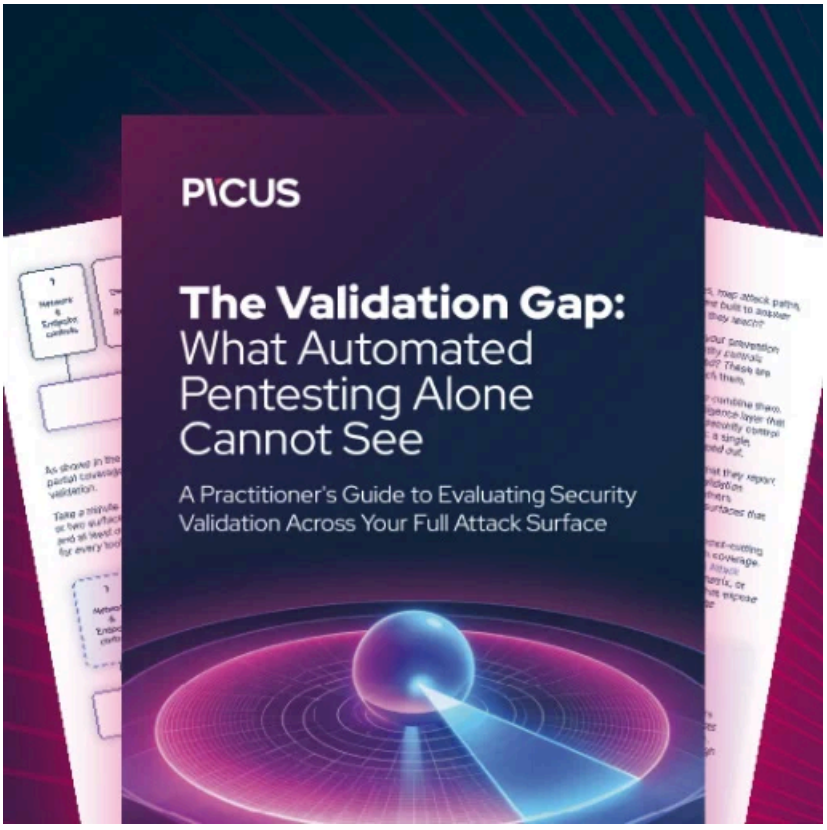
The above commands are executed using system calls retrieved dynamically from the 'libc' library, and the outputs are written to temporary files for reporting.



Simplified attack flow
Source: Claroty

Given IOCONTROL targets' role in critical infrastructure and the group's continuous activity, Claroty's report constitutes a valuable resource for defenders to help identify and block the threat.

The complete indicators of compromise (IoC) are listed at the bottom of the report.



Automated Pentesting Covers Only 1 of 6 Surfaces.

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: https://www.bleepingcomputer.com/news/security/new-iocontrol-malware-used-in-critical-infrastructure-attacks/