Threat Group Cards: A Threat Actor Encyclopedia

Archived: 2026-04-05 18:33:37 UTC

Home > List all groups > List all tools > List all groups using tool IOCONTROL

Tool: IOCONTROL

Names	IOCONTROL
Category	Malware
Type	ICS malware
Description	(Claroty) Team82 obtained a sample of a custom-built IoT/OT malware called IOCONTROL used by Iran-affiliated attackers to attack Israel- and U.S.-based OT/IoT devices. IOCONTROL has been used to attack IoT and SCADA/OT devices of various types including IP cameras, routers, PLCs, HMIs, firewalls, and more. Some of the affected vendors include: Baicells, D-Link, Hikvision, Red Lion, Orpak, Phoenix Contact, Teltonika, Unitronics, and others. We've assessed that IOCONTROL is a cyberweapon used by a nation-state to attack civilian critical infrastructure.
Information	<https://claroty.com/team82/research/inside-a-new-ot-iot-cyber-weapon-iocontrol> <https://therecord.media/us-offers-reward-for-iran-hacker-iocontrol-malware>

Last change to this tool card: 28 June 2025

Download this tool card in JSON format

All groups using tool IOCONTROL

Changed	Name	Country	Observed	
Unknown groups				
	[Interesting malware not linked to an actor yet]			

1 group listed (0 APT, 0 other, 1 unknown)