

Threat Hunt Report

Hussain Syed Naqvi

7/20/2025

CIS 3213 Cybersecurity Foundations

Ryan Irving

1. Threat Actor Review

Threat Actor Name: CyberAv3ngers

Associated Group(s): Islamic Republic of Iran; associated with the Islamic Revolutionary Guard Corps (IRGC) group known as Soldiers of Soloman

Targeted Industry/Sector: Critical infrastructure, especially water systems, ICS/SCADA, and energy sectors

Motivations: Political, religious, ideological, and disruptive (hacktivism supporting Iranian geopolitical aims)

Summary of Notable Campaigns or Attacks:

- The CyberAv3ngers have been known to be active since at least 2020, with disputed and false claims of critical infrastructure compromises in Israel.
- In 2023, the CyberAv3ngers engaged in a global targeting and hacking of the Unitronics Programmable Logic Controller (PLC) with Human-Machine Interface (HMI). This PLC can be found in multiple sectors, including water and wastewater, energy, food and beverage manufacturing, and healthcare. The most notable feature of this attack was the defacement of the devices user interface.

2. MITRE ATT&CK Mapping and Navigator Usage

I reviewed the MITRE ATT&CK page for CyberAv3ngers (G1027) and used the ICS mapping provided to identify and visualize the techniques they use. I referenced the techniques already highlighted by MITRE based on CyberAv3ngers' Unitronics Defacement Campaign.

Provided is a screenshot I took of the MITRE ATT&CK which displays the relevant techniques used by CyberAv3ngers. These include:

Initial Access 12 techniques	Execution 10 techniques	Persistence 6 techniques	Privilege Escalation 2 techniques	Evasion 7 techniques	Discovery 5 techniques	Lateral Movement 7 techniques	Collection 11 techniques	Command and Control 3 techniques	Inhibit Response Function 14 techniques	Impair Process Control 5 techniques	Impact 12 techniques
Drive-by Compromise	Autosun Image	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection Enumeration	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing Application	Change Operating Mode	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote Services	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote Services	Command-Line Interface	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application Layer Protocol	Block Command Message	Spoof Reporting Message	Denial of View
External Remote Services	Execution through API	Project File Infection		Masquerading	Remote System Information Discovery	Lateral Tool Transfer	Data from Local System		Block Reporting Message	Unauthorized Command Message	Loss of Availability
Internet Accessible Device	Graphical User Interface	System Firmware		Rootkit	Wireless Sniffing	Program Download	Detect Operating Mode		Block Serial COM		Loss of Control
Remote Services	Hooking	Valid Accounts		Spoof Reporting Message		Remote Services	I/O Image		Change Credential		Loss of Productivity and Revenue
Replication Through Removable Media	Modify Controller Tasking			System Binary Proxy Execution		Valid Accounts	Monitor Process State		Data Destruction		Loss of Protection
Rogue Master	Native API						Point & Tag Identification		Denial of Service		Loss of Safety
Spearphishing Attachment	Scripting						Program Upload		Device Restart/Shutdown		Loss of View
Supply Chain Compromise	User Execution						Screen Capture		Manipulate I/O Image		Manipulation of Control
Transient Cyber Asset							Wireless Sniffing		Modify Alarm Settings		Manipulation of View
Wireless Compromise									Rootkit		Theft of Operational Information
									Service Stop		
									System Firmware		

Click [here](#) to access the JSON File

T-ID	Technique Name	Use in Campaign
T0812	Default Credentials	Exploited hardcoded/default credentials (e.g., 1111) on Unitronics PLC HMIs.
T0814	Denial of Service	Defaced HMIs and disrupted pumping station communications.

T0883	Internet Accessible Device	Targeted PLCs/HMIs exposed to the public internet, often via vulnerable modems.
T0826	Loss of Availability	Rendered PLCs and HMIs inoperable, halting business operations.
T0828	Loss of Productivity and Revenue	Downtime impacted multiple industrial sectors' operational output.
T0829	Loss of View	Replaced HMI screens, obscuring process visibility for operators.

3. Detection and Threat Hunting Strategy

CyberAv3ngers (G1027) primarily targets Industrial Control Systems (ICS), particularly engaging in global targeting and hacking of the Unitronics Programmable Logic Controller (PLC) with Human-Machine Interface (HMI), using tactics such as default credentials, defacement, and disruptions. This was demonstrated in their Unitronics Defacement Campaign back in November 2023. Because their techniques involve exploiting weak authentication and misconfigured devices, defenders can implement proactive detection and threat hunting across both IT and OT networks.

Detection Strategy for ICS-targeting threats (CyberAv3ngers):

- Monitor login attempts to PLCs and HMIs for default or repeated credentials
- Alert on access to ICS systems from unknown or external IP addresses
- Use tools like Shodan or Censys to find exposed Unitronics devices
- Watch for changes to HMI screens or unexpected PLC configurations
- Detect device unavailability or control system failures linked to unauthorized access
- Review logs for sudden loss of visibility, requiring manual intervention

Tools and Data Sources:

- SIEM (Splunk, Elastic)
- OT monitoring (Claroty, Nozomi)
- Network monitoring (Zeek, Suricata)
- PLC/HMI logs, firewall logs, SNMP traps
- Shodan/Censys (for public exposure scans)

4. Conclusion

The threat hunt on CyberAv3ngers (G1027) demonstrates their focused campaign on targeting internet-exposed industrial control systems (ICS), particularly Unitronics PLCs and HMIs. The group exploited default credentials, public access points, and denial-of-service tactics to disrupt operations, deface interfaces, and cause significant downtime across multiple sectors.

Some of their key techniques included exploitation of default passwords, defacement of HMI displays, and loss of system visibility and availability. These low-complexity but high-impact methods demonstrate the need for basic ICS security enhancements/upgrades.

Recommended next steps:

1. Immediately change all default passwords on ICS devices and use strong, encrypted credentials.
2. Conduct external scans to identify internet-exposed control systems. Spread awareness amongst cybersecurity teams of these security gaps.
3. Implement strict access controls and firewall rules for all OT networks.
4. Monitor abnormal device behavior, login attempts, and HMI changes across the network.
5. Deploy OT-aware monitoring tools (such as Nozomi or Claroty) to detect future threats.

Improving visibility, reducing exposure, and applying proactive monitoring are important in order to protect critical infrastructure from groups like CyberAv3ngers.

5. References

MITRE ATT&CK Group G1027: CyberAv3ngers.

<https://attack.mitre.org/versions/v17/groups/G1027/>

Dragos. *CyberAv3ngers: Hactivist Group Targeting Israel-Made OT Devices*.

<https://www.dragos.com/blog/cyber-av3ngers-hactivist-group-targeting-israel-made-ot-devices/>