Hive Pro

Threat Level

Red

CISA: AA26-097A

Hiveforce Labs

THREAT ADVISORY

ATTACK REPORT

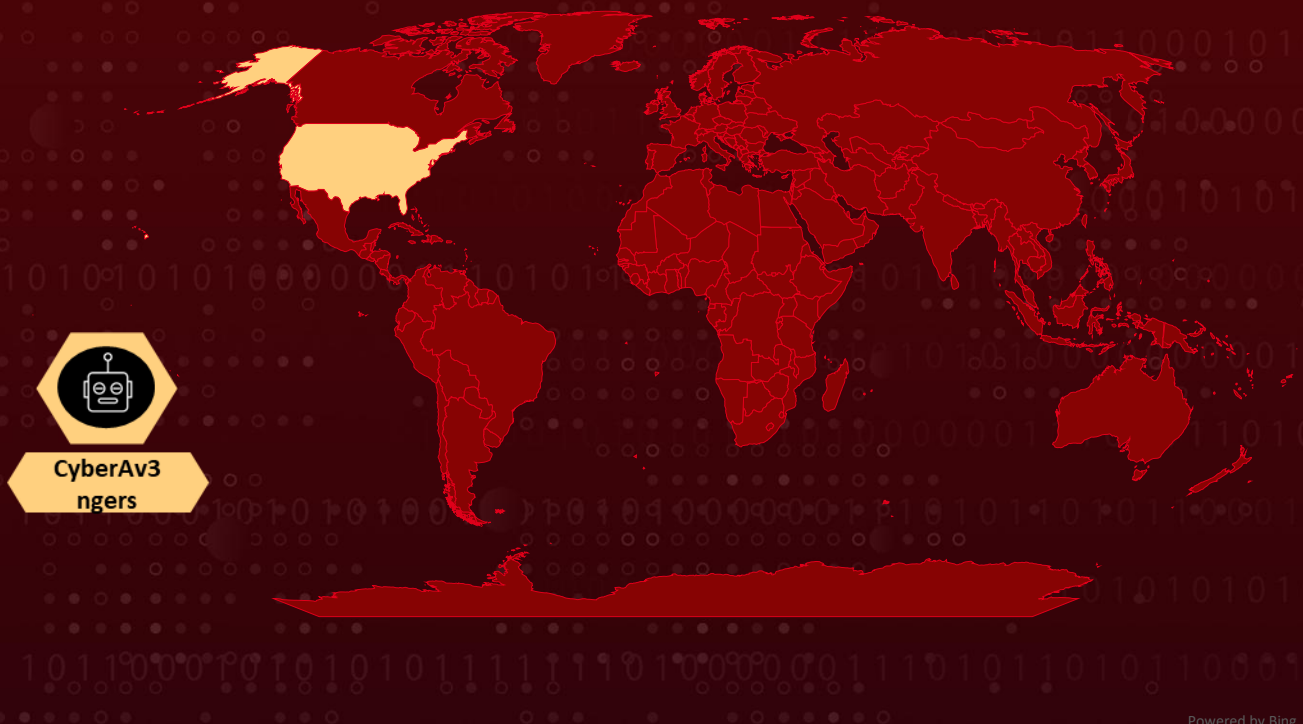
Iranian-Affiliated CyberAv3ngers Exploits Internet-Exposed PLCs in U.S.

Date of Publication	Admiralty Code	TA Number
April 09, 2026	A1	TA2026094

Summary

Attack Commenced: March 2026
Targeted Regions: United States
Targeted Platforms: Operational Technology (OT) / Industrial Control Systems (ICS), Windows-based HMI/SCADA systems
Targeted Products: Rockwell Automation CompactLogix PLCs, Micro850 PLCs, Rockwell Automation Studio 5000 Logix Designer, RSLogix 5000
Targeted Industries: Government, Water and Wastewater Systems (WWS), Energy
Threat Actor: CyberAv3ngers (aka Hydro Kitten, Shahid Kaveh Group, UNC5691, Storm-0784)
Attack: CyberAv3ngers, an Iranian-affiliated threat group, targeted internet-exposed Rockwell Automation PLCs across U.S. critical infrastructure sectors by exploiting CVE-2021-22681 to bypass authentication and establish accepted PLC connections via leased third-party infrastructure. Following initial compromise, the actors deployed Dropbear SSH on victim endpoints to maintain persistent remote access and extracted PLC project files while manipulating data on HMI and SCADA displays, causing operational disruption and financial loss.

Attack Regions



CVE

CVE	NAME	AFFECTED PRODUCT	ZERO-DAY	CISA KEV	PATCH
CVE-2021-22681	Rockwell Multiple Products Insufficient Protected Credentials Vulnerability	Rockwell Automation Studio 5000 Logix Designer Versions 21 and later and RSLogix 5000: Versions 16 through 20	✗	✓	✓

Attack Details

#1

CyberAv3ngers, an Iran-affiliated cyber actor, is targeting internet-facing operational technology (OT) devices across critical infrastructures in the U.S., including programmable logic controllers (PLCs). CyberAv3ngers gained initial access by exploiting CVE-2021-22681, a CIP (Common Industrial Protocol) Security authentication bypass vulnerability affecting Rockwell Automation Studio 5000 Logix Designer (versions 21 and later) and RSLogix 5000 (versions 16 through 20). The flaw allows an unauthenticated attacker to bypass the key-based verification mechanism used when communicating with Rockwell Automation CompactLogix and ControlLogix controller families.

#2

Operating from leased, third-party hosted infrastructure and using legitimate Rockwell Automation configuration software, the threat actors crafted accepted connections to internet-exposed CompactLogix and Micro850 PLC devices deployed within government facilities, Water and Wastewater Systems, and energy sector environments. The use of leased infrastructure and legitimate tooling was a deliberate effort to reduce attribution overhead and blend activity into expected industrial communications traffic.

#3

After achieving initial access to the PLC environment, the actors moved to establish persistent remote access by deploying Dropbear, a lightweight Secure Shell (SSH) software, directly on victim endpoints. Dropbear was configured to listen on port 22, giving the threat actors a reliable, encrypted remote channel for ongoing command-and-control operations. Using the persistent remote access provided by Dropbear SSH, the threat actors proceeded to interact with the PLC project file, the authoritative configuration artifact governing PLC logic and behavior, and manipulated display data presented on Human-Machine Interface (HMI) and Supervisory Control and Data Acquisition (SCADA) panels.

#4

These actions directly undermined the situational awareness of operators monitoring industrial processes. The manipulation of SCADA display data is a particularly disruptive capability in OT environments, as operators rely on accurate display readings to make safety-critical decisions. In multiple cases, these actions resulted in diminished PLC functionality, operational disruption, and documented financial loss across the targeted sectors.

#5

The broader campaign context links CyberAv3ngers and associated Iranian threat actors including MuddyWater operating under the TAG-150 umbrella to a coordinated cyber influence and operational ecosystem aligned with Iran's Ministry of Intelligence and Security (MOIS). ChainShell and Tsundere (aka Dindoor) are assessed as co-deployed components of the TAG-150 platform, frequently delivered alongside CastleRAT. Public-facing domains and Telegram channels serve as primary amplification and C2 infrastructure for this ecosystem, enabling the malware to communicate with threat actor-controlled bots while blending in with legitimate platform traffic and reducing infrastructure overhead. The campaign represents a deliberate, accelerating pattern of Iranian offensive cyber activity targeting both IT and OT infrastructure across Western and Israeli entities.

Recommendations

Remove PLCs from Internet Exposure: Immediately audit all OT network perimeters and ensure no PLC devices, especially Rockwell Automation CompactLogix and Micro850 units, are directly reachable from the internet. Place PLCs behind dedicated industrial firewalls or network proxies that strictly control which hosts can initiate connections.

Patch CVE-2021-22681 on Affected Rockwell Automation Devices: Apply available firmware and software updates for Rockwell Automation Studio 5000 Logix Designer and RSLogix 5000 to remediate the CIP Security authentication bypass. Consult Rockwell Automation's Security Advisory portal for device-specific guidance and minimum patched version requirements.

Disable Remote Modification of PLC Logic: Enable physical and/or software-based write-protection switches on CompactLogix and Micro850 controllers to prevent unauthorized modification of the PLC project file. Confirm that only explicitly authorized engineering workstations can push logic changes, and enforce this through both network ACLs and the controller's own key-switch settings.

Hunt for Dropbear SSH and ChainShell Indicators: Conduct immediate threat hunts across OT-adjacent and IT environments for Dropbear SSH binaries listening on port 22, the PowerShell script "reset.ps1", and any JavaScript execution activity on hosts that do not normally run scripts. Review process creation logs, PowerShell transcripts, and network logs for outbound connections to Ethereum RPC nodes or smart contract addresses.

Monitor HMI and SCADA Displays for Unauthorized Changes: Establish integrity baselines for HMI screen configurations and SCADA data display templates. Implement alerting for any unauthorized modification to display tags, process variable bindings, or alarm setpoints. Cross-reference SCADA display data against raw sensor readings to detect discrepancies indicative of display manipulation.

Disable Unused Authentication Features on PLC Devices: Review and disable all unused or legacy authentication features on Rockwell Automation controllers that could weaken the overall security posture. Ensure that the CIP Security configuration reflects least-privilege principles and that only required communication paths are permitted.

Potential MITRE ATT&CK TTPs

Tactic	Technique	Sub-technique
Initial Access	T1190: Exploit Public-Facing Application	
	T1078: Valid Accounts	
Execution	T1059: Command and Scripting Interpreter	T1059.001: PowerShell
		T1059.007: JavaScript
Persistence	T1133: External Remote Services	
Command and Control	T1102: Web Service	
	T1571: Non-Standard Port	
Collection	T1005: Data from Local System	
Impact	T1565: Data Manipulation	T1565.001: Stored Data Manipulation
	T1489: Service Stop	

Indicators of Compromise (IOCs)

TYPE	VALUE
Filename	reset.ps1
IPv4	135[.]136[.]1[.]133, 185[.]82[.]73[.]162, 185[.]82[.]73[.]164, 185[.]82[.]73[.]165, 185[.]82[.]73[.]167, 185[.]82[.]73[.]168, 185[.]82[.]73[.]170, 185[.]82[.]73[.]171

Patch Link

https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.PN1550.html

References

https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a

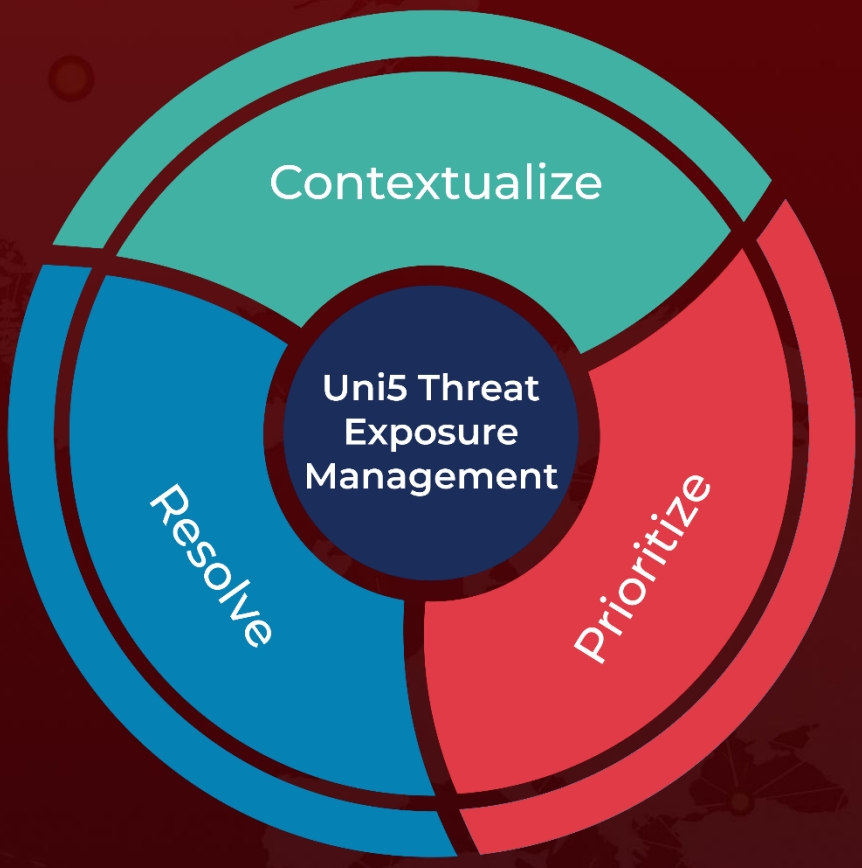
https://www.cisa.gov/sites/default/files/2026-04/AA26-097A-Iranian-Affiliated-Cyber-Actors-Exploit-Programmable-Logic-Controllers-Across-US-Critical-Infrastructure_508c.pdf

https://hivepro.com/threat-advisory/iranian-apt-group-cyberav3ngers-target-u-s-critical-infrastructure/

What Next?

At **Hive Pro**, it is our mission to detect the most likely threats to your organization and to help you prevent them from happening.

Book a free demo with **HivePro Uni5**: Threat Exposure Management Platform.



REPORT GENERATED ON

April 09, 2026 • 08:30 AM

More at www.hivepro.com