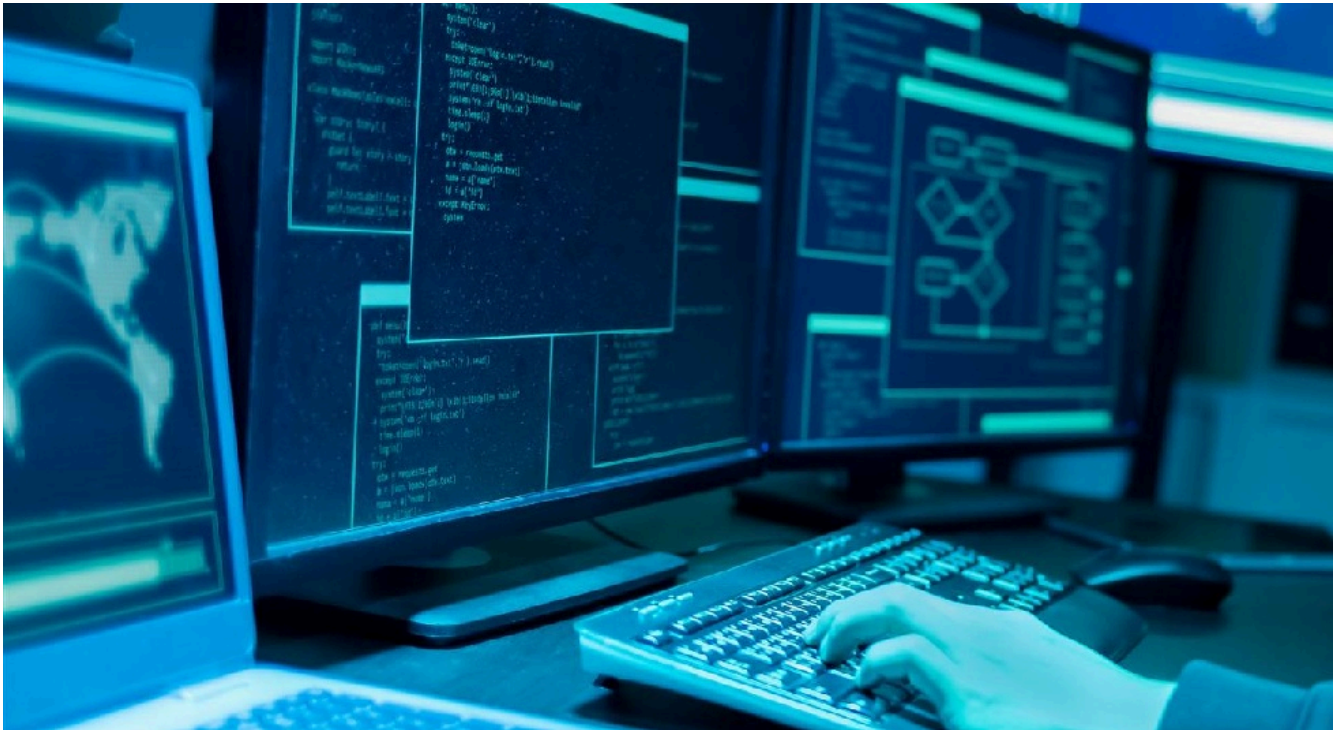


Federal Agencies Warn of Ongoing PLC Exploitation Against Critical U.S. Infrastructure

 trendmicro.com/en_us/research/26/g/plc-exploitation.html

July 23, 2026



Key takeaways

- Multiple federal agencies updated their joint CISA advisory, warning that attackers manipulated operator displays so personnel couldn't visually detect anything was amiss on their screens.
- The attackers scanned the internet for exposed PLCs and connected using legitimate engineering software, the same way an authorized technician would.
- The July 2026 update widens the manufacturer scope beyond Rockwell Automation / Allen-Bradley to include Schneider Electric and Siemens equipment, and adds detection guidance for malicious changes hidden in shared, reusable code modules.
- Unlike a similar but largely disruption-free campaign in 2023, this ongoing activity has caused confirmed operational disruption and financial loss for some affected organizations.
- Targeted sectors include government facilities, water systems, and energy infrastructure across the U.S.
- The TrendAI Vision One™ platform detects and blocks the indicators of compromise (IoCs) associated with this activity, listed at the end of this entry.

Six federal agencies have just updated an advisory about ongoing attacks on the equipment that physically runs U.S. critical infrastructure, including city services, water plants, and power facilities. The advisory, first issued in April 2026 and revised on July 22, warns that attackers are actively targeting these systems.

The activity involves attackers scanning the internet for exposed industrial control systems (ICS) and connecting to them using legitimate engineering software, the same way an authorized technician would. Once inside, they alter the controllers' underlying logic, the instructions that tell the equipment what to do. In some cases, they also change what's shown on the operators' screens. The attacks are built specifically so the humans in the loop can't spot any anomalies on their screens.

The joint advisory, [AA26-097A](#), is cosigned by the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the Environmental Protection Agency (EPA), the Department of Energy, and U.S. Cyber Command. It warns that nation-state and advanced persistent threat (APT) actors are actively exploiting internet-facing programmable logic controllers (PLCs) across U.S. government services, water systems, and energy infrastructure.

What is a PLC and why is this physical?

A PLC is a specialized, ruggedized industrial device built to run the control logic that operates physical equipment. It replaced the banks of hardwired electromechanical relays that once did this job, swapping fixed wiring for logic that can be reprogrammed. It's what opens the valve, starts the pump, holds the pressure, and trips the breaker.

A PLC runs its control logic on the device itself, so it drives the physical process with or without a network connection. What makes the ongoing activity possible is that many are also reachable over a network, and that reach is what the attackers exploit.

Two other terms significant to this incident are the following:

- **Project file:** The blueprint that tells the controller how to operate. On Rockwell Automation / Allen-Bradley equipment, it's a binary .ACD file, built in Studio 5000 Logix Designer, that stores much more than the logic alone: the ladder logic plus the tag database, I/O and controller configuration, and overall program structure. In simple terms, it holds rules like "if pressure exceeds the limit, close the valve," but it captures the whole operating setup, not just individual rules.
- **Human-machine interface (HMI):** The screens operators watch to see what the equipment is doing and to control it.

Held together, these three make the core of the ongoing exploitation easy to describe: The attackers reach the controllers, copy the blueprint, and change what the humans see. A real industrial environment is far more than these three pieces—it includes mechanical processes that no PLC controls and steps that still depend on people—but this narrow slice is exactly what the attackers manipulate.

How this differs from the 2023 attacks

In November 2023, a group affiliated with the Iranian IRGC Cyber Electronic Command (IRGC-CEC), known as CyberAv3ngers (also tracked as Hydro Kitten, Shahid Kaveh Group, and Storm-0784), [compromised at least 75 PLCs](#) in U.S. water facilities. Those devices were running default credentials, so it was a simple problem with a simple fix: Change the password.

Short of formally naming the same group, the federal agencies describe activity in the ongoing attacks that is consistent with the 2023 attacks. The current exploitation is more sophisticated in three specific ways:

- Better tooling: Instead of default passwords, the actors use Rockwell's own Studio 5000 Logix Designer, legitimate engineering software with working credentials. From the network's point of view, the connection looks like a solid job done by a technician.
- Wider scope: The advisory's original April 2026 publication centered on Rockwell Automation / Allen-Bradley CompactLogix and Micro850 controllers. The July 2026 update widens that scope to include Schneider Electric and Siemens PLCs, along with other brands.
- Real consequences: The 2023 campaign was largely disruption-free, whereas the ongoing exploitation has produced confirmed operational disruption and financial loss for some victim organizations.

The advisory update also flags a quieter but serious risk: malicious changes hidden inside reusable code modules, shared blocks of logic dropped into many PLC programs at once. Because a tampered module carries its changes into every process that reuses it, a single edit can spread across an entire operation. That turns an operator's own engineering library, full of trusted configuration standards and specs, into a supply-chain problem, which is exactly what the update's new detection guidance is meant to catch.

No vulnerability required

Traffic tied to the ongoing activity showed up on five ports:

- 22 (SSH)

- 102 (ISO-TSAP, primarily used by Siemens STEP 7 and the S7comm protocol, though other protocols such as ICCP also run over it)
- 502 (Modbus TCP)
- 2222 (EtherNet/IP implicit messaging, runs over UDP for time-critical I/O)
- 44818 (EtherNet/IP explicit messaging, TCP only, used for configuration and diagnostics; primarily associated with Rockwell Automation / Allen-Bradley, though other vendors such as Wago use it too)

None of that traffic depends on a software bug. The threat actors scan for internet-exposed PLCs and connect to them the same way a legitimate engineer would. That is an architectural weakness, not a patchable one, because these controllers are deployed without sufficient network segmentation, authentication gating, or remote-access hardening. Public scan data from Shodan shows more than [74,000 ICS devices](#) directly reachable from the open internet today—down from a level that held [around 120,000](#) for much of the period since 2017—and many still run default or no credentials at all.

Security recommendations

Defending against these attacks is largely a matter of configuration and access control, so it requires no new hardware or lengthy procurement cycle and can begin immediately. The steps below move from what to do this week, to what to fix this quarter, to what the industry itself owes operators and organizations.

What to do this week

- **Remove PLCs from direct internet exposure.** Route all remote access through a secure gateway or jump host with multifactor authentication (MFA), and ensure cellular modems used for field connectivity are authenticated and logged.
- **Use physical mode switches where available.** Set hardware key switches to RUN and only move to PROGRAM or REMOTE during active, supervised maintenance windows. On some controllers, the switch position can still be overridden by a network command, so it works best as one layer alongside removing internet exposure and gating remote access.
- **Search logs for the published indicators.** Query firewall, intrusion detection system, and network monitoring logs for the advisory IP addresses on ports 22, 102, 502, 2222, and 44818, with attention to traffic from overseas hosting providers.

What to fix this quarter

- **Enable programming protection on software key switches.** Rockwell operators should follow the current [SD1771 guidance](#); Siemens operators should [configure protection](#) in TIA Portal.
- **Back up PLC logic and configurations offline, and test restores.** Store backups on secured physical media, separate from the network the PLC lives on.
- **Harden beyond the immediate response.** Enforce MFA on all operational technology (OT) remote access, block unnecessary OT ports at the perimeter, disable unused services like Telnet and default web interfaces, and monitor continuously for configuration changes against a known-good baseline.

Pushing accountability to vendors

The advisory doesn't put all of this on operators. It presses manufacturers directly: Ship products that don't expose administrative interfaces to the internet by default, support MFA (including phishing-resistant methods), and stop charging extra fees for the basic security features that a product needs to run safely. Organizations [buying industrial equipment](#) should make these firm conditions of purchase and get them written into the contract.

Validating continuously

When the intrusion method involves legitimate software and valid credentials, a point-in-time assessment reveals almost nothing about whether an environment stays protected next month. The advisory's own recommendation is to validate these controls continuously, rather than check them once. Knowing what's reachable from the internet into the OT environment and confirming that segmentation is enforced rather than assumed is the whole difference between reading the advisory and acting on it.

TrendAI Vision One™ Threat Intelligence Hub

[TrendAI Vision One™ Threat Intelligence Hub](#) provides the latest insights on emerging threats and threat actors, exclusive strategic reports from TrendAI™ Research, and TrendAI Vision One™ Threat Intelligence Feed in the [TrendAI Vision One™](#) platform.

Emerging Threats: [Federal Agencies Warn of Ongoing PLC Exploitation Against Critical US Infrastructure](#)

TrendAI Vision One™ Intelligence Reports (IoC Sweeping)

[Federal Agencies Warn of Ongoing PLC Exploitation Against Critical US Infrastructure](#)

TrendAI Vision One™ XDR Data Explorer App

Customers using TrendAI Vision One™ can use the XDR Data Explorer App to match the malicious indicators covered in this blog article against data in their own environments for hunting purposes.

CyberAv3ngers C&C infrastructure connections

| eventSubId:201 AND dst:("185.82.73.175" OR "141.11.164.153" OR "175.110.121.42" OR "175.110.121.39" OR "175.110.121.107" OR "185.225.17.225" OR "79.133.46.209" OR "88.80.150.199" OR "88.80.150.200" OR "88.80.150.202" OR "185.82.73.162" OR "185.82.73.164" OR "185.82.73.165" OR "185.82.73.167" OR "185.82.73.168" OR "185.82.73.170" OR "185.82.73.171" OR "135.136.1.133")

CyberAv3ngers C&C DNS resolution

| eventSubId:301 AND hostName:(*tylarion867mino.com* OR *ocferda.com*)

Indicators of compromise

The indicators of compromise (IoCs) listed below are sourced from CISA. These are detected and blocked by the TrendAI Vision One™ platform.

URLs and IP addresses

IoC	Detection
185.82.73[.]175	91 - C&C server
141.11.164[.]153	91 - C&C server
175.110.121[.]42	91 - C&C server
175.110.121[.]39	91 - C&C server
175.110.121[.]41	38 - Computers/Internet
175.110.121[.]107	91 - C&C server
192.142.54[.]79	38 - Computers/Internet
84.200.205[.]165	38 - Computers/Internet

185.225.17[.]225	91 - C&C server
79.133.46[.]209	91 - C&C server
88.80.150[.]199	91 - C&C server
88.80.150[.]200	91 - C&C server
88.80.150[.]202	91 - C&C server
185.82.73[.]162	91 - C&C server
185.82.73[.]164	91 - C&C server
185.82.73[.]165	91 - C&C server
185.82.73[.]167	91 - C&C server
185.82.73[.]168	91 - C&C server
185.82.73[.]170	91 - C&C server
185.82.73[.]171	91 - C&C server
135.136.1[.]133	91 - C&C server
ocferda[.]com	91 - C&C server
uuokhhfsdlk[.]tylarion867mino[.]com	91 - C&C server
tylarion867mino[.]com	91 - C&C server

File hashes

IoC	Detection
366e435a1ea0f597deb6ebe7c0c5acdb6e8b33eb	Backdoor.Linux.IOCONTROL.CIGBCBF
95bd07b4400095acdafce05888da27228d7d07ca	Trojan.Win64.MALPDB.A