ARC SITUATION REPORT · TLP:CLEAR

Iranian-Affiliated APT Targeting of Rockwell/Allen-Bradley PLCs

Internet Exposure Assessment in Response to CISA Advisory AA26-097A

PUBLISHED	April 7, 2026	**ADVISORY**	CISA AA26-097A
DATA SOURCE	Censys Internet Map	**TRAFFIC LIGHT**	TLP:CLEAR
HOSTS IN SCOPE	5,219 globally	**SECTORS**	WWS, Energy, Gov. Facilities

On April 7, 2026, the FBI, CISA, NSA, EPA, DOE, and U.S. Cyber Command jointly disclosed ongoing exploitation of internet-facing Rockwell Automation/Allen-Bradley programmable logic controllers (PLCs) by Iranian-affiliated APT actors. Censys data identifies **5,219 internet-exposed hosts** globally responding to EtherNet/IP (EIP) and self-identifying as Rockwell Automation/Allen-Bradley devices — the attack surface directly relevant to AA26-097A. The United States accounts for 74.6% of global exposure (3,891 hosts), with a disproportionate share on cellular carrier ASNs indicative of field-deployed devices on cellular modems. Censys pivoting of the published IOC list reveals that CISA's seven 185.82.73.x indicators represent **a single multi-homed Windows engineering workstation** running the full Rockwell toolchain, with **four additional operator IPs on the same host absent from the advisory.**

1. THREAT CONTEXT

The authoring agencies assess that a group of Iranian-affiliated APT actors — linked to the IRGC Cyber Electronic Command (CEC) and previously tracked as **CyberAv3ngers** (Shahid Kaveh Group, Storm-0784, Bauxite, UNC5691) — has been conducting targeted exploitation of internet-facing Rockwell Automation/Allen-Bradley PLCs since at least March 2026. This activity follows a similar campaign beginning November 2023 that compromised at least 75 Unitronics devices across U.S. water and wastewater facilities (CISA AA23-335A).

The current campaign involves direct access to internet-exposed PLCs using legitimate vendor software (Rockwell Studio 5000 Logix Designer), enabling actors to interact with project files and manipulate HMI/SCADA display data without requiring zero-day exploitation. Confirmed targeted device families include **CompactLogix** and **Micro850**. The advisory notes additional OT protocols (Modbus/502, S7/102) are also being probed, suggesting broader multi-vendor targeting intent.

2. GEOGRAPHIC EXPOSURE

Censys identifies 5,219 internet-exposed hosts globally responding to EtherNet/IP (port 44818) and self-identifying as Rockwell Automation/Allen-Bradley devices. Geographic distribution is heavily skewed toward the United States, which accounts for 74.6% of global exposure — consistent with Rockwell's dominant market position in North American industrial automation.

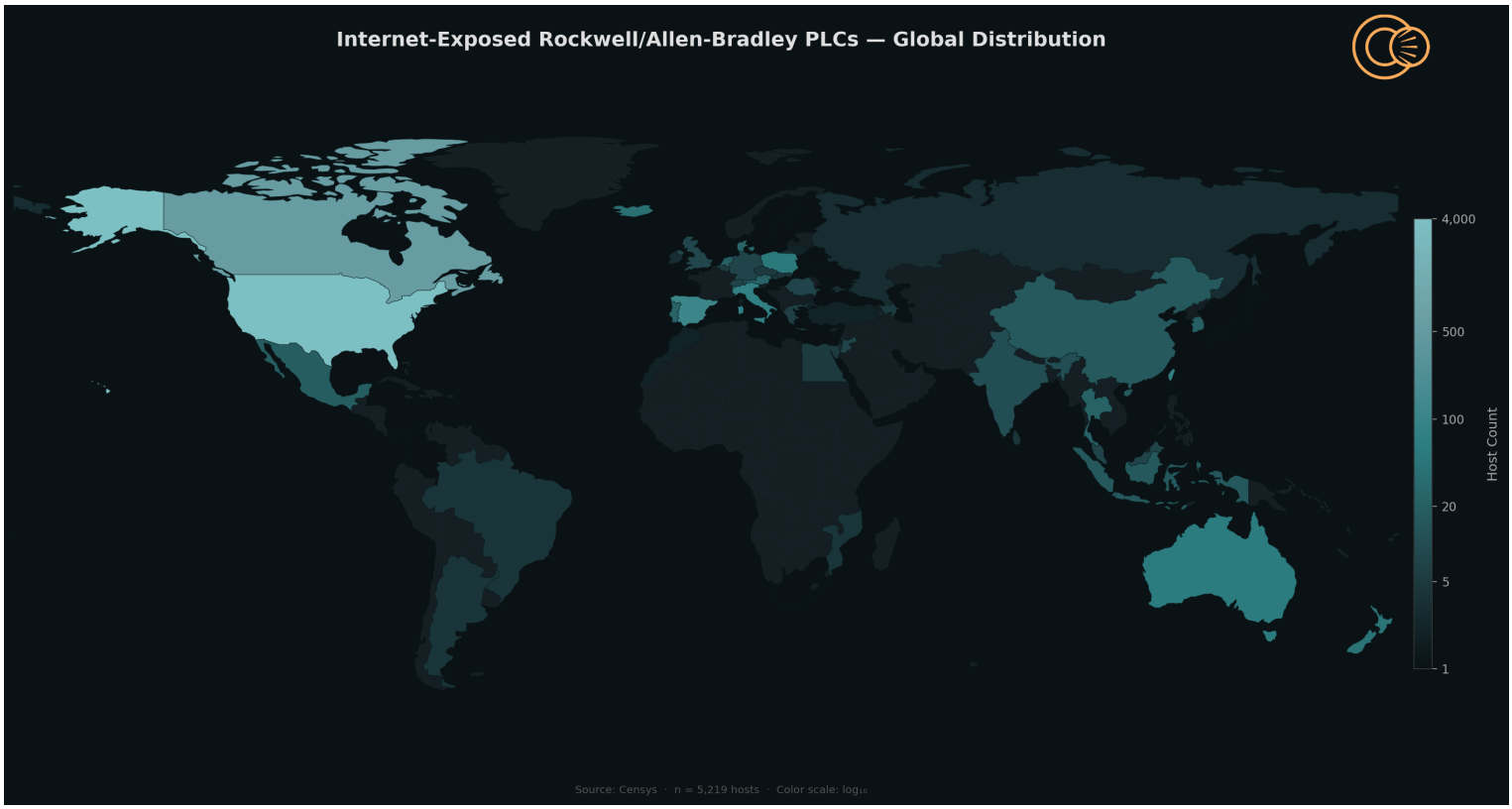

Figure 1. Global distribution of internet-exposed Rockwell/Allen-Bradley PLC hosts (Censys, April 7, 2026).

Key geographic observations: Spain (110), Taiwan (78), and Italy (73) represent the largest non-Anglosphere concentrations. Iceland's presence (36 hosts) is disproportionate to its population and warrants attention given its geothermal energy infrastructure. The advisory specifically targets U.S. Government/Facilities, WWS, and Energy sectors — all with strong domestic Rockwell footprints.

3. AUTONOMOUS SYSTEM ANALYSIS

The ASN distribution of exposed devices reveals a striking concentration on **cellular carrier networks**, with Verizon Business (CELLCO-PART) alone accounting for 2,564 hosts (49.1% of global total) and AT&T Mobility adding a further 693 (13.3%). This pattern strongly indicates that a large fraction of internet-exposed PLCs reach the internet via cellular modems used for remote field connectivity — a deployment pattern the advisory explicitly flags as requiring hardening.

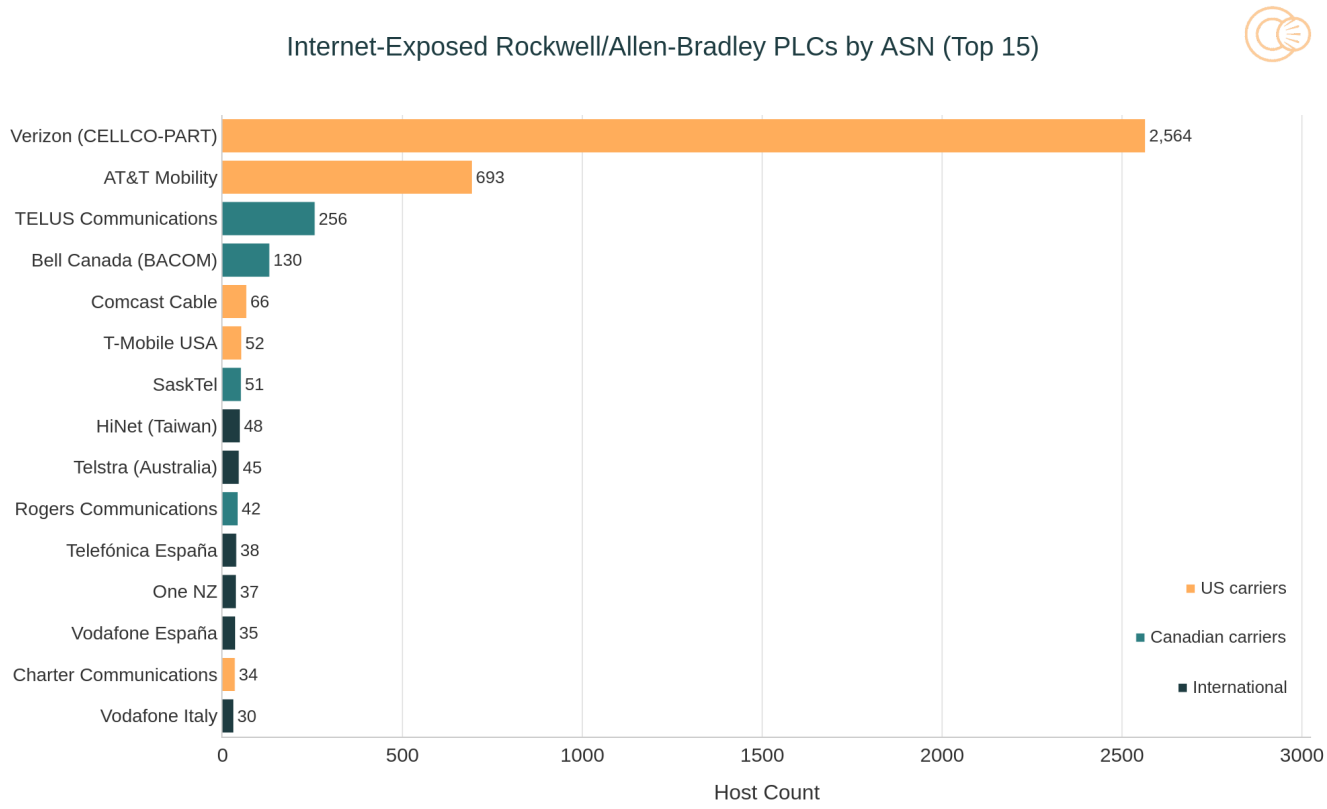

Figure 2. Top 15 ASNs hosting internet-exposed Rockwell/Allen-Bradley PLCs.

The dominance of consumer/business cellular ASNs (Verizon, AT&T, T-Mobile, Charter, Comcast) over industrial or datacenter ASNs is operationally significant: these devices are almost certainly field-deployed in physical infrastructure (pump stations, substations, municipal facilities) with cellular modems as their sole internet path. SPACEX-STARLINK's presence (24 hosts) reflects the broader trend of satellite-connected ICS devices that are difficult to monitor and patch.

4. DEVICE PRODUCT BREAKDOWN

EtherNet/IP identity responses expose device-level product strings, enabling granular fingerprinting of PLC model and firmware revision without authentication. The top 15 product strings are dominated by two families: **MicroLogix 1400** (catalog prefix 1766-) and **CompactLogix** (1769-, 5069-), with one Micro820 (2080-) entry.

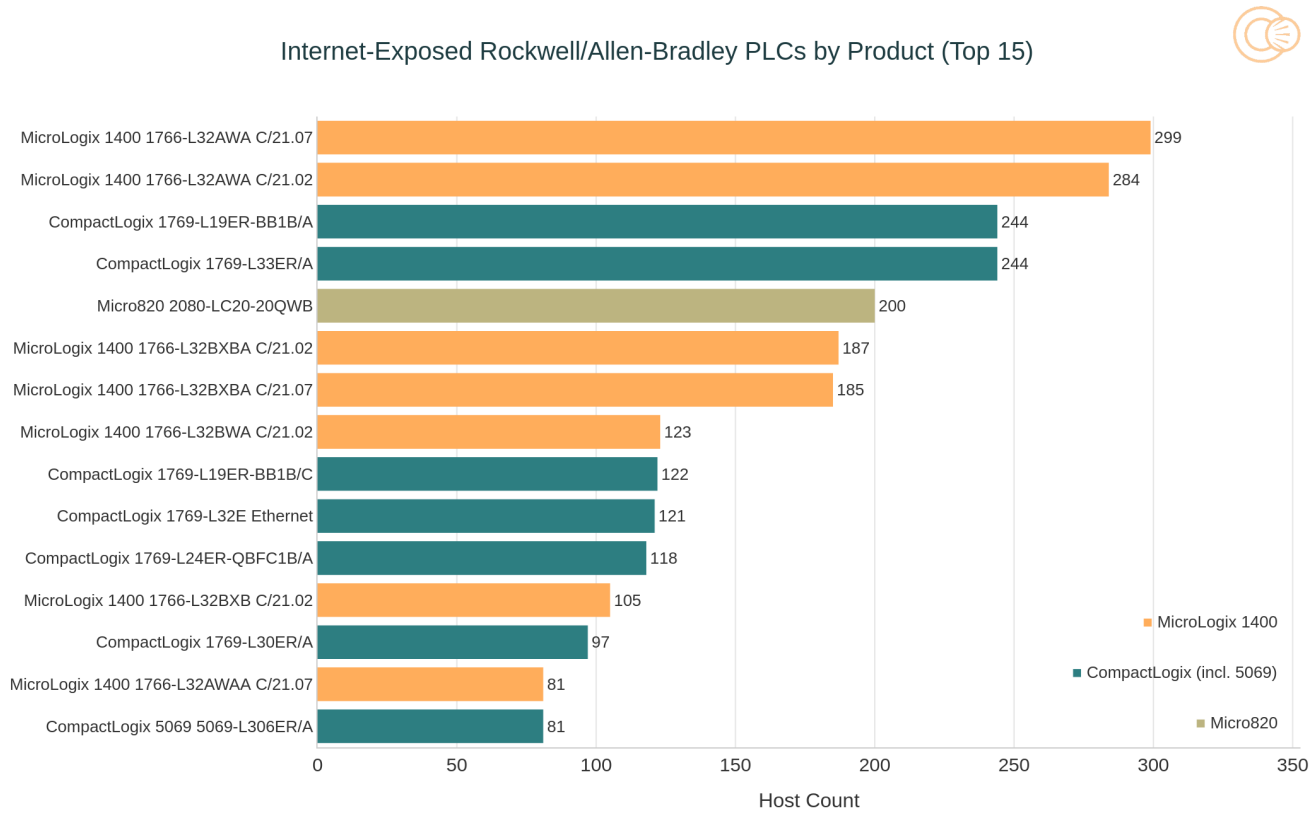

Figure 3. Top 15 product strings among internet-exposed Rockwell/Allen-Bradley hosts.

The advisory specifically names **CompactLogix and Micro850** as confirmed targeted families. The heavy MicroLogix 1400 presence — many running end-of-sale firmware C/21.02 and C/21.07 — is a compounding risk: limited ongoing security support, and firmware version strings embedded unauthenticated in every EIP identity response, allowing actors to enumerate and prioritize unpatched devices at scan time.

5. CO-EXPOSED SERVICES & ATTACK SURFACE AMPLIFIERS

Censys protocol enumeration across the 5,219-host population reveals significant co-exposure of additional services beyond EIP/44818. These services expand the available attack surface and in several cases represent direct paths to operational impact independent of PLC exploitation.

Protocol / Service	Services
HTTP/HTTPS (web interface)	**7,770**
VNC (remote desktop)	**771**
SSH	**530**
FTP	**473**
SNMP	**418**
Modbus	**292**
Telnet	**280**
Red Lion Crimson	**256**

Table 1. Co-exposed protocols on Rockwell/Allen-Bradley PLC hosts (Censys, April 7, 2026).

Notable findings: VNC (771 service instances) represents direct remote desktop access to HMI workstations — precisely the vector described in AA26-097A for SCADA display manipulation. Telnet (280) is a cleartext legacy protocol with no place on internet-facing OT infrastructure. Modbus (292) alongside EIP confirms multi-protocol OT exposure consistent with the advisory's observation that actors are probing Modbus/502. Red Lion Crimson (256) indicates hybrid multi-vendor deployments on the same network segment.

6. IOC ANALYSIS & OPERATOR INFRASTRUCTURE

CISA's advisory ships with eight indicator IPs. Censys pivoting of those indicators into infrastructure data changes the picture in two material ways: the seven 185.82.73.x IPs represent **one multi-homed Windows engineering workstation**, not seven separate hosts; and **four additional operator IPs on that same machine are absent from the advisory.** The eighth indicator, 135.136.1.133, is a distinct single-use staging box with separate infrastructure and a different operational profile.

6.1 The Operator Workstation: 185.82.73.160–.171 (AS214036, ULTAHOST)

Every IP in the 185.82.73.0/24 cluster shares a consistent fingerprint: RDP on non-standard TCP port 43589, backed by a self-signed certificate with common name `DESKTOP-BOE5MUC`. The same Windows machine name appearing across multiple distinct IPs is a high-fidelity operator marker. The hosts also expose a full Windows protocol stack (DCERPC/135, MSMQ, NetBIOS). On .165, .167, and .168, Censys observed a Rockwell EIP listener returning:

```
vendor_name = "Rockwell Software, Inc." vendor_id = 0x004d product_name = "DESKTOP-BOE5MUC" device_type = "Communications Adapter"
```

A real Allen-Bradley PLC never reports a Windows hostname as its product name. This is **RSLinx / FactoryTalk Linx running on the operator workstation itself**, stamping the machine name into its CIP identity response. On .164, a WebAdmin dashboard served by MS .NET Remoting and a WIBU CodeMeter HTTP endpoint — the license daemon shipped with Rockwell FactoryTalk — further confirm the full Rockwell engineering toolchain (Studio 5000, FactoryTalk, RSLinx, CodeMeter) is installed. These IPs are not victims and not honeypots. They are the operators' own launch pad.

Pivoting the RDP certificate. Searching `cert.parsed.subject.common_name="DESKTOP-BOE5MUC"` returned 22 unique self-signed certificates. Walking each through host observation history yielded **11 IPs across 185.82.73.160–.171** (with

.169 currently dark). Four of these — .160, .161, .163, and .166 — do not appear in the advisory. Same Windows image, same RDP/43589, same cert family, same activity window. All are confirmed in AS214036 (ULTAHOST-AS, Amsterdam) as of today.

One host, not eleven VMs. Certificate `2dd70440…` (validity Feb–Aug 2025) was served simultaneously across all 11 IPs. Nine stopped serving it on 2025-07-09 within a ten-second window:

```
185.82.73.162 / .163 / .164 / .165 / .168 / .170 / .171 → 2025-07-09 08:46 UTC 185.82.73.166 → 2025-07-09 09:41 UTC 185.82.73.161 → 2025-07-09 19:38 UTC
```

Eleven independent VMs do not regenerate RDP certificates in the same second. A single Windows host with RDP bound to multiple interfaces does, because one service restart rotates the certificate across every interface simultaneously. A second certificate (`156523d0…`, Dec 2025–Jun 2026) repeats the pattern across .160 and .168. The data fits **one Windows host in AS214036, multi-homed across .160–.171**, active continuously from January 2025 through March 2026.

6.2 The Staging Box: 135.136.1.133 (AS9009, M247 Romania)

The eighth IOC sits in M247 Europe Romania (AS9009) and is unrelated to the .73.x cluster by every available signal: different ASN, different cert family, no RDP/43589, different JA4T fingerprint, and a different leaked Windows hostname. Where the .73.x workstation leaks `DESKTOP-BOE5MUC` (Windows client) through every service it exposes, .133 leaks `WIN-U4IRECQ65UN` — a default Windows Server hostname baked into a stock VPS template that ships without sysprep.

The /24 (135.136.1.0/24) was carved out of an old NCR Voyix allocation and reassigned to M247 Romania on **2026-01-21**. The host first appeared 2026-02-23 — a freshly-provisioned /24 rented within a month of becoming available. Its service timeline is tightly clocked and entirely deliberate:

Date / Time (UTC)	Event
`2026-02-23 19:35`	**DCERPC/135 up — host first appears, bare Windows shell**
`2026-03-14 06:03`	EIP/44818 up
`2026-03-15 01:36`	HTTP/8082 up
`2026-03-15 08:34`	EIP/44818 down (~26h active lifetime)
`2026-03-15 11:32`	WinRM/5985 up
`2026-03-16 19:18–19:40`	HTTP/22350, TCP/3060, TCP/27000 up (22-min burst)
`2026-03-17 09:35–20:34`	DCERPC, WinRM, TCP/3060, HTTP/22350, TCP/27000 all down
`2026-03-18 03:47`	**HTTP/8082 down — host effectively dark**

Table 2. Service lifecycle of 135.136.1[.]133 (Censys historical observation).

A 19-day idle period (bare Windows shell), then a 26-hour EIP test, then a 22-minute burst in which three services come up simultaneously on Mar 16, all tear down within 24 hours of each other almost to the minute — a scheduled-task signature, not a human cleaning up — then a coordinated full teardown on Mar 17–18. The full active window is **approximately four days (Mar 14–18)**, matching CISA's March-only association window exactly. This is a **single-use staging box**: provisioned weeks ahead, activated for one operation, then abandoned. CISA's attribution must come from victim-side telemetry; there are no operator-unique fingerprints to extend from this host.

6.3 Expanded IOC Table

The table below consolidates all confirmed operator infrastructure. The four rows highlighted in red are absent from the published advisory but share the same workstation, ASN, certificate family, and activity window as the named IOCs. **185.82.73.169 is currently dark but is the most likely missing twelfth interface** — check historical logs for traffic. All indicators defanged for safe distribution.

Indicator	CISA IOC?	ASN	First Seen	Last Seen
`135.136.1[.]133`	Yes	AS9009 / M247 Romania	Feb 2026	Mar 2026
`185.82.73[.]160`	**NO – NEW**	AS214036 / ULTAHOST	Apr 2025	Mar 2026
`185.82.73[.]161`	**NO – NEW**	AS214036 / ULTAHOST	Mar 2025	Mar 2026
`185.82.73[.]162`	Yes	AS214036 / ULTAHOST	Mar 2025	Mar 2026
`185.82.73[.]163`	**NO – NEW**	AS214036 / ULTAHOST	Mar 2025	Mar 2026
`185.82.73[.]164`	Yes	AS214036 / ULTAHOST	Mar 2025	Mar 2026
`185.82.73[.]165`	Yes	AS214036 / ULTAHOST	Mar 2025	Mar 2026
`185.82.73[.]166`	**NO – NEW**	AS214036 / ULTAHOST	Jun 2025	Mar 2026
`185.82.73[.]167`	Yes	AS214036 / ULTAHOST	May 2025	Mar 2026
`185.82.73[.]168`	Yes	AS214036 / ULTAHOST	May 2025	Mar 2026
`185.82.73[.]170`	Yes	AS214036 / ULTAHOST	Jun 2025	Mar 2026
`185.82.73[.]171`	Yes	AS214036 / ULTAHOST	Jun 2025	Mar 2026

Table 3. Full expanded IOC list. Red rows = operator IPs absent from CISA AA26-097A, identified via Censys RDP certificate pivot. ASN data confirmed April 7, 2026.

7. PRIORITY MITIGATIONS

The following actions are drawn from AA26-097A and prioritized by Censys exposure data. Items marked IMMEDIATE should be addressed before end of business today.

- **[IMMEDIATE]** Remove PLCs from direct internet exposure. All remote access must be mediated through a jump host or secure gateway. Disable cellular modems if remote access is not operationally required.
- **[IMMEDIATE]** For CompactLogix and MicroLogix devices with a physical mode switch, place the switch in RUN position. This is the only control surface CIP cannot override remotely, and the headline mitigation for this threat.
- **[IMMEDIATE]** Query logs for inbound traffic on TCP 44818, 2222, 102, 502, and 22 from all IPs in Table 3 — including the four newly identified operator addresses (.160, .161, .163, .166). Treat the entire 185.82.73.160–.171 range in AS214036 as suspect.
- **[HIGH]** Disable or firewall VNC, Telnet, and FTP on any host co-located with a PLC. Censys data shows 453 hosts with VNC and 260 with Telnet exposed — direct HMI access paths consistent with SCADA manipulation described in the advisory.
- **[HIGH]** Implement MFA for all remote OT network access, including via VPN and cellular modem management interfaces.
- **[MEDIUM]** Audit MicroLogix 1400 deployments on firmware C/21.02 and C/21.07. End-of-sale devices with limited patch support and unauthenticated firmware version exposure should be prioritized for replacement or network isolation.
- **[MEDIUM]** Monitor EIP identity responses for unexpected firmware version changes, which may indicate project file modification by a threat actor.

8. THREAT HUNTING QUERIES

The following Censys queries enable forward-looking detection of operator infrastructure expansion and victim-side exposure. The first two are high-precision operator markers; new results in either are a leading indicator of renewed or expanding activity.

Operator workstation: RDP certificate family

```
cert.parsed.subject.common_name="DESKTOP-BOE5MUC"
```

New certificates in this family indicate the operator is expanding or rebuilding engineering infrastructure. Any new host serving this cert should be treated as active threat actor capacity.

Operator workstation: Rockwell engineering software on Windows

```
host.services.eip.identity.vendor_id="0x004d" and host.services.eip.identity.product_name=/DESKTOP-.+/
```

Rockwell vendor ID 0x004d combined with a Windows-style hostname in the EIP product_name field identifies RSLinx / FactoryTalk Linx on an exposed Windows host. Healthy ICS networks do not produce this signal.

Operator workstation: exposed CodeMeter license daemons

```
web.endpoints.http.headers:(key="Server" and value="WIBU-SYSTEMS HTTP Server")
```

WIBU CodeMeter is the license daemon shipped with Rockwell FactoryTalk. Internet-exposed instances are a strong marker for engineering workstations running the full Rockwell toolchain.

Victim-side exposure: reproduce this report

```
(host.services.protocol=EIP) and host.services.eip.identity.vendor_name= "Rockwell Automation/Allen-Bradley"
```

Returns all 5,219 internet-exposed Rockwell/Allen-Bradley hosts globally. Append "and host.location.country_code=US" to filter to the 3,891 U.S. hosts.