ALERTA TÉCNICA

TLP:GREEN

MICITT-DC-CSIRT-AT-394-2026

Explotación activa de PLCs por actores APT vinculados a Irán

Se comunica a los directores(as) y jefes(as) de Tecnologías de Información para que tomen las consideraciones necesarias ante la detección de actividad maliciosa dirigida a dispositivos industriales tipo PLC (Programmable Logic Controllers), atribuida a actores APT vinculados a Irán.

Investigaciones recientes confirman la explotación activa de PLCs en infraestructuras críticas, principalmente en sectores como energía, agua, manufactura y servicios gubernamentales. Estas actividades han provocado interrupciones operativas y pérdidas financieras, evidenciando un riesgo elevado para organizaciones que dependen de tecnología operacional (OT).

Los actores identificados están asociados a grupos como “CyberAv3ngers” (también conocidos como Hydro Kitten o Storm-0784), vinculados al IRGC Cyber Electronic Command, quienes han demostrado capacidades para comprometer sistemas industriales mediante accesos remotos, explotación de vulnerabilidades conocidas y uso de infraestructura maliciosa distribuida.

Capacidades técnicas observadas

Los actores presentan las siguientes capacidades:

- Explotación de PLCs expuestos directamente a internet.
- Uso de accesos remotos inseguros hacia sistemas OT.
- Abuso de vulnerabilidades conocidas en dispositivos industriales.
- Interrupción de procesos físicos controlados por PLCs.
- Uso de infraestructura distribuida para el escaneo y explotación.
- Movimientos laterales entre entornos IT y OT.
- Generación de impacto operativo y financiero en las víctimas.

Contexto de la amenaza

Durante labores de monitoreo e inteligencia de amenazas, se ha identificado una campaña activa dirigida a sistemas de control industrial (ICS), específicamente PLCs, utilizada por actores APT vinculados a Irán. Esta actividad ocurre en un contexto de tensiones geopolíticas, donde históricamente estos actores han priorizado ataques disruptivos contra infraestructura crítica.

La evidencia indica que múltiples sectores han sido afectados, incluyendo servicios de agua, energía, tecnología, educación y gobierno local, con presencia de actividad en diversas regiones. Los ataques han resultado en interrupciones operativas reales, lo que confirma la capacidad de estos actores para impactar procesos físicos.

Los PLCs representan un objetivo crítico debido a que, en muchos entornos, carecen de controles de seguridad modernos, presentan exposición directa a internet o mantienen conexiones inseguras con redes IT. Esto facilita su explotación mediante técnicas relativamente simples pero efectivas.

El compromiso de estos dispositivos puede derivar en afectaciones significativas, incluyendo interrupción de servicios esenciales, manipulación de procesos industriales y daños económicos. En este contexto, se recomienda reforzar de manera urgente las medidas de seguridad en entornos OT y validar los indicadores de compromiso asociados.

MITRE ATT&CK Techniques:

Acceso Inicial
• T1190 – Explotación de aplicaciones expuestas públicamente

Persistencia / Movimiento Lateral
• T1021 – Servicios remotos
• T0886 – Acceso remoto a dispositivos de control

Evasión de defensas
• T0814 – Manipulación de controladores industriales

Impacto
• T0827 – Interrupción de procesos
• T0831 – Manipulación de control

Comando y Control
• T0885 – Comunicación remota en sistemas ICS

Indicadores de Compromiso (IOCs):

Direcciones IP maliciosas

185.93.89[.]10
192.253.248[.]180
141.98.11[.]230
141.98.11[.]194
92.209.211[.]41
175.110.121[.]39
185.82.73[.]175
175.110.121[.]42
175.110.121[.]107
185.82.73[.]171
185.82.73[.]170
185.82.73[.]168
185.82.73[.]167
185.82.73[.]165
185.82.73[.]164
185.82.73[.]162
135.136.1[.]133

Puertos asociados a entornos OT/PLC

44818 (EtherNet/IP)
2222
102 (Siemens S7)
502 (Modbus)

Recomendaciones:

- Eliminar la exposición directa de PLCs a internet mediante el uso de firewalls y gateways seguros.
- Segmentar adecuadamente las redes OT de las redes IT.
- Restringir el acceso remoto únicamente a conexiones seguras y controladas.
- Monitorear tráfico hacia puertos industriales (44818, 2222, 102, 502), especialmente desde direcciones externas.
- Aplicar parches de seguridad a dispositivos y software asociados a PLCs.
- Revisar logs en busca de actividad anómala o conexiones sospechosas.
- Implementar soluciones de monitoreo continuo y detección de anomalías en entornos OT.
- Seguir las recomendaciones de fabricantes (ej. configuraciones seguras en controladores).
- Fortalecer controles de acceso y autenticación en sistemas industriales.

Referencias:

- Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), National Security Agency (NSA), & partner agencies. (2026). Iranian-affiliated cyber actors targeting programmable logic controllers (PLCs). https://www.cisa.gov/news-events/cybersecurity-advisories/aa26-097a
- Cisco Talos Intelligence Group. (2026). Iranian adversaries exploiting PLCs. Cisco Talos Intelligence Bulletin.
- Rockwell Automation. (2026). Security advisory SD1771: Guidance for PLC protection. https://www.rockwellautomation.com/en-us/trust-center/security-advisories/advisory.SD1771.html
- MITRE Corporation. (2025). ICS techniques in MITRE ATT&CK® for Industrial Control Systems. https://attack.mitre.org/matrices/ics/

En caso de alguna duda o consulta, se pueden comunicar al CSIRT-CR por medio del correo electrónico csirt@micitt.go.cr

JASON CASTRO MARTINEZ (FIRMA)
Fecha: 2026.04.15 17:45:46 -06'00'

Analista de Ciberseguridad

JOSE ALONSO ROCHA VILLALOBOS (FIRMA)
Firmado digitalmente por JOSE ALONSO ROCHA VILLALOBOS (FIRMA)
Fecha: 2026.04.15 17:49:06 -06'00'

Analista de Ciberseguridad