IT Digital Magazine Última edición Descárgatela

La tensión geopolítica dispara el riesgo cibernético sobre infraestructuras críticas y entornos OT

- Seguridad

29 MAY 2026

El nuevo WatchGuard Geopolitical Cyber Report analiza la actividad del grupo iraní CyberAv3ngers contra PLC y sistemas industriales. El informe identifica más de 5.200 dispositivos expuestos a Internet y advierte de que los ataques OT pueden afectar a procesos físicos esenciales.

WatchGuard Technologies ha publicado el WatchGuard Geopolitical Cyber Report, un nuevo análisis de inteligencia que examina cómo el aumento de las tensiones internacionales está elevando de forma directa el riesgo cibernético sobre infraestructuras críticas. El informe, elaborado por el equipo del SOC de la compañía, pone el foco en la actividad de CyberAv3ngers, un grupo vinculado a Irán que ha intensificado sus ataques contra controladores lógicos programables (PLC) y entornos de tecnología operacional (OT) en Norteamérica, provocando interrupciones operativas, manipulación de pantallas HMI/SCADA y pérdidas económicas en organizaciones afectadas.

El informe señala además que los atacantes han utilizado herramientas legítimas de ingeniería para conectarse a los sistemas, lo que dificulta la detección mediante mecanismos tradicionales centrados en malware.

Aunque el estudio se centra en Norteamérica, WatchGuard advierte de que las tácticas observadas son relevantes para cualquier organización con sistemas OT expuestos a Internet, incluidos mercados como España.

El ciberespacio como frente de tensión internacional

El informe sitúa estos ataques en un contexto global marcado por la escalada geopolítica. Tras los últimos episodios analizados, se registraron 1.245 ciberataques asociados a 99 actores de amenaza y 14 países, lo que evidencia la creciente conexión entre crisis internacionales y ofensivas digitales.

Una de las conclusiones clave es que los ataques contra entornos OT ya no deben interpretarse como incidentes informáticos convencionales. WatchGuard subraya que estas campañas pueden afectar directamente a procesos físicos, alterando el funcionamiento de bombas, válvulas, líneas de producción o sistemas de suministro. El compromiso de un PLC puede tener consecuencias operativas y de continuidad de servicio, especialmente en sectores esenciales.

La investigación identifica 5.219 hosts expuestos a Internet que responden a EtherNet/IP. Aunque la mayoría se encuentran en Estados Unidos, el informe detecta también presencia en otros países, entre ellos España, con 110 dispositivos, además de Taiwán e Italia. Los sectores potencialmente afectados incluyen sistemas de agua y aguas residuales, infraestructuras energéticas, servicios e instalaciones gubernamentales y sectores manufactureros y dependientes de OT.

La investigación concluye que cualquier organización con tecnología OT accesible desde la red pública debe considerarse dentro del alcance potencial de esta amenaza.

TAGS

CONTENIDO RELACIONADO

- La probabilidad de que una infraestructura crítica española sufra un ataque grave supera el 60%

- El hacktivismo se convierte en una herramienta sofisticada de desestabilización geopolítica
- El volumen de ciberataques aumenta un 42% en un año