Encabeza México riesgos por correo malicioso

Por el Staff de El Inversionista

América Latina continúa siendo una de las regiones más vulnerables a los ciberataques dirigidos contra la infraestructura industrial

De acuerdo con el más reciente análisis de Kaspersky ICS CERT, 20.4 por ciento de las computadoras que operan Sistemas de Control Industrial (ICS, por sus siglas en inglés) registró afectaciones por objetos maliciosos, una proporción superior al promedio mundial de 19.7 por ciento, que además representa el nivel más bajo de riesgo global desde 2022.

El estudio coloca a la región como la segunda más expuesta a amenazas perimetrales en el mundo, reflejando que las organizaciones latinoamericanas aún enfrentan importantes desafíos para proteger la tecnología operativa (OT) que controla procesos críticos en sectores como energía, manufactura, construcción e infraestructura.

Uno de los principales focos de preocupación es el correo electrónico, que continúa siendo la puerta de entrada favorita para los ciberdelincuentes.

Kaspersky detectó que 5.3 por ciento de las computadoras industriales de la región fue afectada por amenazas distribuidas mediante este canal, una incidencia equivalente a 1.9 veces el promedio global.

Eduardo Chavarro, director para América del Equipo Global de Respuestas a Incidentes de Kaspersky, explicó que los indicadores confirman que el correo electrónico continúa siendo el eslabón más explotado por los atacantes para comprometer la tecnología operativa.

«El uso de documentos maliciosos y spyware no busca causar un daño inmediato, sino obtener un acceso inicial de forma sigilosa. Una vez que consiguen credenciales válidas, los actores maliciosos pueden desplazarse lateralmente por las redes corporativas hasta llegar a los sistemas de control de procesos críticos, incrementando significativamente el riesgo de incidentes operativos o de ataques de ransomware», señaló.

México sobresale como el país con mayor nivel de exposición

El 9.51 por ciento de las computadoras industriales mexicanas registró afectaciones derivadas de correos maliciosos, la tasa más alta de América Latina, seguido por Uruguay con 8.56 por ciento.

En contraste, Colombia, Brasil, Argentina y Chile permanecen dentro de los niveles habituales observados para la región.

En América Latina, 3.08 por ciento de los equipos industriales fue impactado por este tipo de amenazas, una cifra 1.8 veces superior a la media mundial.

Nuevamente, México encabezó el listado con una tasa de afectación de 5.28 por ciento, apenas por encima de Uruguay, que registró 5 por ciento.

El reporte también advierte un crecimiento de los ataques mediante scripts maliciosos y páginas de phishing, diseñados para robar credenciales y datos de autenticación del personal. En este rubro, la tasa regional alcanzó 9.65 por ciento de las computadoras ICS.

Panamá fue el caso más sobresaliente, al registrar una afectación de 18.24 por ciento, impulsada por un incremento de campañas dirigidas a comprometer sitios gubernamentales desarrollados sobre WordPress.

El análisis sectorial muestra que las industrias con mayor actividad maliciosa bloqueada en sus sistemas de control fueron biometría, con 27.1 por ciento de equipos afectados; automatización de edificios, con 22.4 por ciento; construcción, con 21.9 por ciento; energía eléctrica, con 19 por ciento; ingeniería e integración de sistemas industriales, con 18.7 por ciento; y manufactura, con 15.7 por ciento.

Ante este panorama, la firma recomienda fortalecer el filtrado y monitoreo del correo electrónico corporativo, segmentar estrictamente las redes de tecnología de la información (TI) y tecnología operativa (OT), restringir el uso de dispositivos USB mediante controles y escaneos de seguridad, capacitar de forma continua al personal para identificar intentos de ingeniería social y phishing, además de implementar soluciones especializadas para la protección de entornos industriales que permitan mejorar la detección y respuesta frente a amenazas avanzadas.

El reporte concluye que, aunque el panorama global muestra una disminución gradual en los incidentes que afectan a los sistemas de control industrial, América Latina aún mantiene una superficie de ataque considerablemente mayor, lo que obliga a las empresas a reforzar sus estrategias de ciberseguridad para proteger la continuidad operativa de infraestructuras consideradas críticas para la economía.