EL MERCURIO DE ANTOFAGASTA

Fecha: 05/07/2025 Audiencia: 17.400 Sección: OPINION
Vpe: $333.226 Tirada: 5.800 Frecuencia: 0
Vpe pág: $1.617.600 Difusión: 5.800
Vpe portada: $1.617.600 Ocupación: 20,6%

Editorial

Ciberataques y la IA

Los cibercriminales están acelerando sus esfuerzos, utilizando IA y automatización para operar a niveles sin precedentes.

Chile recibió 27.600 millones de intentos de ciberataques en 2024, frente a los 6.000 millones del año 2023, según datos dados a conocer hace unos días por FortiGuard Labs, el laboratorio de análisis e inteligencia de amenazas de Fortinet.

Los datos revelan que los actores de amenazas están utilizando de manera exponencial la automatización, las herramientas mercantilizadas e inteligencia artificial (IA) para erosionar de manera sistemática las ventajas antes sostenidas por los defensores. El reporte sobre el panorama global de amenazas de 2025 deja en claro que los cibercriminales están acelerando sus esfuerzos, utilizando IA y automatización para operar a niveles sin precedentes de rapidez y escala, dijo la empresa.

Ésta es una tendencia global ya que se observa una menor cantidad de ataques masivos y un mayor volumen de explotaciones únicas y variantes nuevas de malware y ransomware, que son mucho más dirigidos. Esto significa que hay menos cantidad de ataques pero son diseñados para objetivos específicos, lo que los vuelve más sofisticados y con mayor posibilidad de éxito si las organizaciones no cuentan con defensas de ciberseguridad actualizadas.

El cibercrimen impulsado por IA está escalando de manera rápida.

Pero el manual tradicional de seguridad ya no es suficiente. El cibercrimen impulsado por IA está escalando de manera rápida: los actores de amenazas están aprovechando la inteligencia artificial para mejorar el realismo del phishing y evadir los controles de seguridad tradicionales, lo que hace que los ciberataques sean más efectivos y difíciles de detectar.

Los expertos indican que ha habido un aumento de este tipo de ataques selectivos a nivel mundial, provocados por bandas organizadas, con conocimientos sofisticados sobre vulnerabilidades, lo que obliga a tener una actitud proactiva en cuanto a la protección de datos para mitigar los riesgos.