La Inteligencia Artificial está acelerando una nueva generación de ciberataques

Los ataques informáticos evolucionan más rápido que nunca. Un nuevo reporte internacional elaborado por una de las grandes empresas dedicadas a la seguridad digital advierte sobre el avance de herramientas basadas en IA, el crecimiento del phishing mediante códigos QR y el resurgimiento de viejas amenazas.

Enrique Garabetyan
27-07-2026 06:30

La inteligencia artificial está **modificando** profundamente el mapa mundial de la **ciberseguridad**. Si hasta hace pocos años era vista principalmente como una herramienta para fortalecer las defensas digitales, ahora también se transformó en un aliado cada vez más sofisticado para los ciberdelincuentes.

El resultado es un escenario en el que los ataques son más rápidos, automatizados y difíciles de detectar, tanto para empresas como para usuarios comunes.

Ese es uno de los principales hallazgos del **ESET Threat Report 2026**, que analiza el **panorama** global durante el primer semestre del año. El informe sostiene que los atacantes comenzaron a incorporar agentes de inteligencia artificial y componentes reutilizables -conocidos como *AI Skills*- para automatizar tareas ofensivas.

Esto no les gusta a los autoritarios
El ejercicio del periodismo profesional y crítico es un pilar fundamental de la democracia. Por eso molesta a quienes creen ser los dueños de la verdad.

Durante el período analizado, los investigadores estudiaron cerca de 900 mil de estos módulos y detectaron decenas de miles de instancias sospechosas y miles directamente maliciosas, una señal del rápido crecimiento de este nuevo ecosistema.

Ahora, amenazas digitales más complejas

La consecuencia es que muchas amenazas tradicionales no desaparecieron: simplemente evolucionaron. El **phishing** continúa siendo una de las principales puertas de entrada para el robo de credenciales, mientras que los programas diseñados para capturar contraseñas, los troyanos bancarios y el **ransomware** siguen expandiéndose gracias a nuevas técnicas de **automatización**.

El uso de la IA permite **personalizar** mensajes fraudulentos, imitar estilos de escritura y generar campañas más convincentes, reduciendo las posibilidades de que las víctimas detecten el engaño.

Entre las modalidades que más crecieron figura el denominado ***quishing***, una variante del phishing que reemplaza los enlaces tradicionales por códigos QR. La víctima escanea el código con el teléfono creyendo acceder a un sitio legítimo, pero termina entregando credenciales o descargando software malicioso. También se consolidan campañas que inducen al propio usuario a ejecutar comandos maliciosos bajo la falsa promesa de solucionar problemas técnicos, una estrategia basada en ingeniería social que explota más a las personas que a las vulnerabilidades informáticas.

El 43% de los usuarios fue hackeado: cuáles son las recomendaciones para prevenirlo

Los dispositivos móviles tampoco escapan a esta tendencia. El informe describe nuevas familias de malware capaces de **interceptar datos bancarios**, aprovechar la tecnología **NFC** o utilizar capacidades de IA para ampliar su alcance. A medida que las **billeteras virtuales**, las aplicaciones financieras y la autenticación mediante el celular se vuelven más frecuentes, los teléfonos inteligentes pasan a ocupar un lugar central en la estrategia de los atacantes.

El fenómeno no preocupa únicamente a los especialistas de ESET. Informes recientes de otras compañías de ciberseguridad coinciden en que la automatización está reduciendo drásticamente los tiempos entre el descubrimiento de una vulnerabilidad y su explotación por parte de delincuentes. Lo que antes podía demorar semanas hoy puede **concretarse en cuestión de horas,** obligando a organizaciones y usuarios a adoptar una actitud mucho más **proactiva** frente a las actualizaciones y las buenas prácticas de seguridad.

Para los expertos, el principal desafío ya no consiste únicamente en desarrollar mejores herramientas de protección, sino también en fortalecer la cultura de la ciberseguridad. Porque, aunque la inteligencia artificial esté transformando el modo en que operan los atacantes, la mayoría de los incidentes sigue comenzando con un error humano: un clic apresurado, una contraseña débil o un mensaje que parecía inofensivo.

Seis hábitos que reducen el riesgo digital

La primera **barrera** de seguridad sigue siendo el usuario. Los especialistas recomiendan mantener siempre **actualizados** el sistema operativo y las aplicaciones; activar la **autenticación** en dos pasos; **utilizar contraseñas largas** y diferentes para cada servicio, preferentemente administradas con un **gestor** de claves; **desconfiar** de mensajes urgentes o inesperados, incluso si parecen provenir de bancos o empresas conocidas; **no escanear códigos QR** de origen **dudoso**; y realizar **copias de seguridad** periódicas de la información importante. Estas medidas simples no eliminan el riesgo, pero reducen significativamente las posibilidades de sufrir un ataque.