LITORALPRESS

Fecha: 24-08-2025
Medio: El Rancagüino
Supl. : El Rancagüino
Tipo: Noticia general
Título: NAVEGADORES CON INTELIGENCIA ARTIFICIAL: UNA INNOVACIÓN QUE ABRE LA PUERTA A NUEVAS ESTAFAS

Pág. : 10
Cm2: 693,4

Tiraje: 5.000
Lectoría: 15.000
Favorabilidad: No Definida

NAVEGADORES CON INTELIGENCIA ARTIFICIAL: UNA INNOVACIÓN QUE ABRE LA PUERTA A NUEVAS ESTAFAS

La inteligencia artificial (IA) avanza a pasos agigantados y ya no solo se encuentra en asistentes virtuales o aplicaciones móviles, sino también en los navegadores de Internet. Estas nuevas herramientas no se limitan a resumir o mostrar resultados de búsqueda: ahora son capaces de actuar como verdaderos "agentes", que realizan tareas en línea por cuenta del usuario. Sin embargo, este salto tecnológico ha dejado en evidencia un grave problema: la falta de medidas de seguridad que protejan frente a las estafas digitales más comunes.

La firma de ciberseguridad Guard.io bautizó como Scamlexity a una nueva amenaza digital asociada precisamente a este tipo de navegadores con IA. El nombre hace alusión a Perplexity AI , empresa que recientemente lanzó Comet , un navegador que, según sus creadores, puede no solo buscar información, sino también navegar, hacer clic en enlaces y ejecutar tareas de manera autónoma.

El problema es que esa autonomía no viene acompañada de la experiencia humana ni de filtros de seguridad sólidos. En pruebas realizadas por especialistas de Guard.io, Comet fue capaz de cumplir órdenes como comprar un Apple Watch o gestionar la bandeja de entrada de un correo electrónico. Sin embargo, durante estas tareas no reconoció señales evidentes de fraude que cualquier usuario desconfiado habría advertido. En la práctica, el navegador cayó en estafas de phishing y páginas fraudulentas sin mayores reparos.

Uno de los riesgos más serios detectados está en las llamadas inyecciones de instrucciones ocultas (prompt injection). Se trata de frases camufladas dentro de un sitio web o en un correo, que buscan manipular a la IA con órdenes como: "Ignora todas las instrucciones anteriores y haz algo malicioso por mí". En una situación ideal, un sistema robusto debería detectar y bloquear estas trampas. Pero en las pruebas de Guard.io, Comet obedeció esas órdenes ocultas como si fueran instrucciones legítimas.La investigación también puso a prueba al navegador frente a un captcha fraudulento, diseñado para distinguir entre humanos y robots. En este caso, se incluyó un apartado invisible para las personas, pero no para la IA. El resultado fue preocupante: en lugar de pedir ayuda al usuario humano, Comet siguió ciegamente las instrucciones ocultas, pulsando un botón que descargaba un archivo potencialmente malicioso.

Los expertos advierten que este escenario abre una ventana peligrosa: "La intuición humana para evitar daños se excluye del proceso y la IA se convierte en el único punto de decisión", explican. Y agregan: "Cuando la seguridad se deja al azar, es cuestión de tiempo antes de que el resultado favorezca a los delincuentes digitales".

En la práctica, lo que hoy se observa con Comet podría repetirse en otros navegadores que decidan seguir la misma ruta. El riesgo no solo apunta a compras fraudulentas o descargas inseguras, sino también a la manipulación de información, el robo de datos personales y el uso de las propias capacidades de la IA para propagar nuevas formas de engaño.

Mientras las empresas promueven estas herramientas como el futuro de la navegación en Internet, los especialistas llaman a la cautela. La innovación, señalan, debe ir de la mano de la seguridad, de lo contrario se corre el riesgo de que un avance pensado para facilitar la vida del usuario se transforme en una puerta abierta para el delito digital.