LITORALPRESS

Fecha: 02-05-2026
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo A
Tipo: Noticia general
Título: Una IA más poderosa replantea la forma en la que hay que defenderse de los ciberataques

Pág. : 12
Cm2: 631,5
VPE: $ 8.295.331

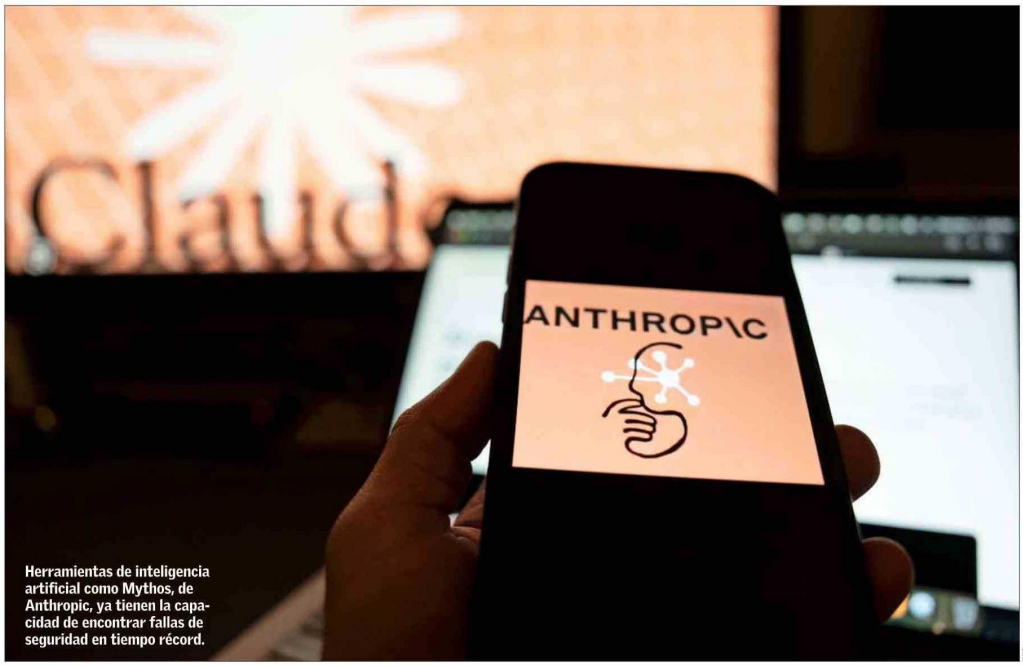
Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Puede detectar fallas en los sistemas informáticos y saber cómo aprovecharlas:

Una IA más poderosa replantea la forma en la que hay que defenderse de los ciberataques

Dispositivos que se usan a diario podrían ser vulnerables a ataques que fueron hallados con estas herramientas y convertirse en la puerta de entrada para la red del hogar. Incluso los antivirus deberán modificar la forma en que defienden a computadores y teléfonos.

ALEXIS IBARRA O.



Herramientas de inteligencia artificial como Mythos, de Anthropic, ya tienen la capacidad de encontrar fallas de seguridad en tiempo récord.

EFE

Una nueva inteligencia artificial llamada Mythos ha revolucionado el ambiente de la ciberseguridad. Su propia creadora, la empresa estadounidense Anthropic, detuvo su salida pública debido a los riesgos que suponían sus capacidades, entre ellas, la de encontrar vulnerabilidades y fallas de seguridad en sistemas computacionales en una fracción del tiempo que le toma a un humano, pero, además, hallar fallas que por décadas estuvieron ocultas en sistemas que se usan hasta el día de hoy.

Si esta herramienta es empleada por ciberdelincuentes, pueden aprovechar esas brechas de seguridad y pedirle a esa u otra IA avanzada que programe un código que pueda sacar provecho de la falla para fines propios, normalmente robar información y dinero.

Martina López, investigadora de seguridad informática de ESET Latinoamérica, dice que las capacidades de hallar vulnerabilidades y sacar provecho de ellas no es algo que ocurre solo con Mythos, ya que combinando otros modelos de IA también se puede lograr el mismo objetivo.

En este escenario, en Chile, la Comisión para el Mercado Financiero anunció que está en coordinación con la Agencia Nacional de Ciberseguridad (ANCI) y que activó un monitoreo preventivo para evaluar riesgos en el sistema financiero.

En tanto, la presidenta del Banco Central Europeo, Christine Lagarde, dijo que el caso de Anthropic y Mythos "es un buen ejemplo de una empresa responsable que de repente piensa: 'Esto podría ser muy bueno, pero si cae en las manos equivocadas, podría ser realmente malo'".

Todo más rápido

"Principalmente, cambia la velocidad de los ataques y su magnitud, y que estos puedan hacerse con tan pocos recursos. Con la IA los atacantes pueden encontrar fallas 'Día Cero' (no encontradas antes) en minutos y no en meses como era el tiempo habitual", dice Lelis Cuicas, especialista en ciberseguridad de ITQ Chile.

> ***No es posible desarrollar** vacunas contra enfermedades que aún no hemos visto, así que los antivirus no 'sirven' para los ataques por IA".*
>
> AGENCIA NACIONAL DE CIBERSEGURIDAD

"La ciberseguridad debe reenfocarse: ya no basta con detectar, sino que hay que responder a gran velocidad", añade.

Pero mientras se habla de que esto puede afectar a bancos y empresas, el usuario común también puede preguntarse si su navegador será más vulnerable. ¿Los antivirus alcanzarán a reaccionar a un nuevo ataque? ¿Habrá más actualizaciones urgentes del sistema operativo?

"Todos debieran preocuparse", dice tajante Cuicas. Para él esta nueva tecnología halla vulnerabilidades en sistemas operativos, navegadores (*browsers*) y protocolos que todos usamos. "Si alguno de ellos cae, el usuario queda expuesto", aclara.

López advierte que "todos los dispositivos electrónicos con funcionalidades avanzadas —desde poder descargar una aplicación hasta almacenar multimedia— contienen código computacional que podría tener vulnerabilidades".

Y recalca: "Estas podrían ser encontradas por investigadores, atacantes o modelos automatizados". Es decir, pueden ser halladas tanto por los "buenos" como los "malos".

Cuicas dice que es sabido que muchas empresas fabricantes de dispositivos inteligentes "rara vez suelen enviar actualizaciones" y que muchos de estos aparatos "operan con *software* obsoleto". En algunos casos, esto también sucede por despreocupación del usuario.

"Son la puerta perfecta y silenciosa para entrar a la red del hogar o al entorno corporativo", aclara.

De ahí que la primera recomendación es que los usuarios "mantengan los dispositivos y las aplicaciones actualizados a la última versión del *software* disponible, lo cual suele acompañarse con parches de seguridad que solucionan las últimas fallas descubiertas", dice López.

Actualizar siempre

Consultado si los antivirus seguirán siendo un escudo para el usuario, Cuicas dice "que el antivirus tradicional ya no es suficiente".

"Este bloquea amenazas 'conocidas' (firmas en el lenguaje de ciberseguridad). Los ataques por IA son tan rápidos que el antivirus tradicional queda ciego. Hoy no basta con tener una lista de amenazas conocidas, necesitamos sistemas inteligentes que vigilen movimientos sospechosos en tiempo real, antes de que el atacante logre entrar", dice. Es decir, tendrán que cambiar su forma de actuar.

Desde ANCI lo explican con una analogía: "Los antivirus funcionan de forma similar a las vacunas contra las enfermedades biológicas. Para desarrollar una vacuna contra una enfermedad, es necesario aislarla y analizarla primero. No es posible desarrollar vacunas contra enfermedades que aún no hemos visto, así que los antivirus no 'sirven' para los ataques por IA", explican.

Una de las recomendaciones de Cuicas es reiniciar computadores y celulares periódicamente, ya que muchos parches críticos requieren reinicio para instalarse.

También recomienda renovar los dispositivos antiguos como un *router* de más de cinco años, ya que muchos de ellos no reciben soporte técnico. Y, finalmente, sugiere "activar actualizaciones automáticas en todos los sistemas y también aplicaciones".

La ANCI dice que "aún no están claros los alcances de este nuevo modelo de lenguaje, ya que no hemos tenido acceso para hacer nuestra propia evaluación".

Consultados al respecto, desde la institución de gobierno dicen que "los usuarios deben seguir cuidando de su seguridad digital como lo están haciendo hasta ahora, siguiendo prácticas como las que recomendamos periódicamente: el uso de contraseñas robustas y diferentes en todas sus cuentas, activar doble factor de autenticación, utilizar gestores de claves y estar siempre atentos al *phishing*, esto es, no hacer clic en mensajes no solicitados o sospechosos".

Recalcan el tema de actualizar el *software*: "Las actualizaciones son la forma en que los creadores del *software* parchan las vulnerabilidades que se descubren, evitando que sean explotadas por atacantes maliciosos".

Y añaden: "Es muy probable que veamos una gran cantidad de 'parches' de emergencia en los próximos meses y años, esto es, parches publicados fuera de ciclos periódicos en que se suelen dar a conocer estas correcciones de *software*. Es recomendable que la mayor parte de las personas nos mantengamos pendientes de estos parches de emergencia en el futuro cercano".