

¿Utilizarán los hackers más IA en los ataques de ransomware en 2025?

Respuesta breve: Sí. Se espera que los atacantes sigan ampliando su uso de la inteligencia artificial, especialmente los modelos de lenguaje de gran tamaño, para hacerse pasar por personas de confianza y manipular a las víctimas para que otorguen acceso o confianza.

Por qué la IA se ha convertido en la favorita de los hackers

Los resultados de búsqueda, los feeds de noticias y las conversaciones cotidianas están ahora saturados de referencias a la IA, y ese mismo entusiasmo se ha apoderado de los ciberdelincuentes. Cuando la mayoría de las personas mencionan la IA, normalmente se refieren a modelos de lenguaje de gran tamaño como los que están detrás de ChatGPT y herramientas similares que pueden imitar de manera convincente la comunicación humana. Los atacantes han reconocido que esta capacidad es extremadamente útil para la ingeniería social. En lugar de depender de correos de phishing genéricos, pueden generar mensajes, voces o conversaciones que se asemejan estrechamente a un colega, proveedor o figura de autoridad real, lo que facilita mucho ganarse la confianza de un objetivo antes de atacar.

Espere tácticas de suplantación más refinadas

La tendencia de cara a 2025 no es que los ataques impulsados por IA sean completamente nuevos, sino que se están volviendo más pulidos y con un enfoque más empresarial. De la misma manera que las empresas legítimas están implementando agentes de ventas impulsados por IA y herramientas de alcance automatizado, los atacantes están perfeccionando sus propias técnicas de suplantación basadas en IA. Esto significa mensajes más convincentes que imitan a jefes, compañeros de trabajo o socios de confianza, todos diseñados para explotar las relaciones laborales de las que la gente depende cada día. El peligro es que una conversación que se siente personal y legítima en realidad puede provenir de un sistema de IA altamente capaz creado para manipular, no para ayudar.

Qué significa esto para la defensa

A medida que estas tácticas de suplantación maduran, las organizaciones deben asumir que los ataques basados en la confianza serán cada vez más difíciles de detectar únicamente por instinto. Verificar las solicitudes a través de canales independientes, en lugar de confiar en un mensaje o llamada tal cual, se vuelve cada vez más importante. Dado que estos ataques están diseñados para eludir el juicio humano, contar con capacidades automatizadas de detección y respuesta, como las integradas en FortressAI de Cyber Crucible, proporciona una capa adicional de protección cuando la ingeniería social logra sortear las defensas de una persona.

<https://player.vimeo.com/video/1046827321?texttrack=es>

[Ver en Vimeo](#) · Subtítulos: English, Français, Español, العربية

Revision #2

Created 2026-07-24 02:16:57 UTC by Dennis Underwood

Updated 2026-08-06 18:35:10 UTC by Dennis Underwood