MásQueSeguridad

20 de abril 2026

LO MÁS RECIENTE

>>> Infiltración Corporativa: Deepfakes en entrevistas de trabajo

Una nueva modalidad de espionaje corporativo está alarmando al sector empresarial. Los ciberdelincuentes están postulándose a empleos remotos de alto nivel utilizando rostros y voces generados por IA (Deepfakes) durante las videollamadas. Una vez contratados y con credenciales de la empresa, aprovechan su acceso interno para robar bases de datos, instalar ransomware o desviar fondos. Las empresas ahora deben implementar protocolos de verificación de identidad biométrica antes de enviar cualquier contrato.

>>> "Prompt Injection": Tu asistente virtual usado en tu contra

A medida que integramos asistentes de IA (como Copilot o Gemini) en nuestros correos y documentos, surge el ataque de "Inyección de Prompts". Un atacante envía un correo con instrucciones ocultas (texto en color blanco o metadatos). Cuando le pides a tu IA que "resuma los correos del día", la IA lee el comando oculto que le ordena, por ejemplo, buscar contraseñas en tu buzón y reenviarlas al atacante sin que lo notes.

>>> Robo de Sesiones: Falsos agentes de soporte hiper-realistas

Los estafadores han dejado de usar humanos en centros de llamadas (Call Centers). Ahora despliegan enjambres de Chatbots de IA que te contactan por WhatsApp alegando un "problema de facturación" con Netflix, Amazon o tu banco. Estos bots no tienen guiones fijos; están entrenados para mantener conversaciones empáticas, responder a tus dudas y guiarte pacientemente a páginas clonadas para robar tus tokens de sesión y evadir la verificación de dos pasos (2FA).