Publicado en Madrid el 22/08/2024

La IA está aumentando la propagación de 'malvertising': malware a través de anuncios digitales

La aplicación de la Inteligencia Artificial a los anuncios está permitiendo la propagación de malware de forma más rápida, según la compañía de ciberseguridad S2 Grupo. Esta técnica se conoce como "malvertising" y se basa en anuncios que piden descargas o introducción de datos personales, así como la oferta de un producto o servicio a un precio realmente llamativo, descuentos desorbitados o, incluso, gratis

La empresa S2 Grupo, especializada en ciberseguridad y ciberinteligencia, ha advertido en un comunicado que el uso de la Inteligencia Artificial, como cualquier otro avance en tecnología, es de gran ayuda para múltiples sectores y, a la vez, acarrea problemas de seguridad digital. "Lo importante aquí no es temer el contexto, lo relevante es conocer dónde están las vías de riesgo, concienciarnos de la importancia del uso seguro de la tecnología y actuar con responsabilidad. El exceso de confianza y el desconocimiento de los posibles peligros en la red continúan siendo una de las principales puertas de acceso para los ciberdelincuentes", ha explicado José Rosell, CEO de S2 Grupo.

El equipo de expertos de la compañía de ciberseguridad ha detallado que algunos tipos de malvertising son: la esteganografía (oculta código malicioso en imágenes o textos), las imágenes políglotas (imágenes que parecen normales, pero contienen malware y además lo ejecutan), el scareware (anuncios falsos que indican que el dispositivo está infectado y generan temor en el usuario), anuncios que ofrecen falsas actualizaciones de software, y las estafas de soporte técnico (hacen creer de nuevo que el dispositivo está infectado y dan un contacto falso de soporte para solucionarlo).

Algunas claves para detectar un posible caso de malvertising es encontrar anuncios que pidan descargas o introducción de datos personales, así como la oferta de un producto o servicio con descuentos desorbitados o, incluso, gratis. Otro ejemplo de esto es cuando aparecen anuncios de antivirus que no se tienen instalados.

Para evitar ser víctima del malvertising, desde S2 Grupo se recomienda reforzar las configuraciones de privacidad y utilizar solo navegadores seguros. En este sentido, hay que instalar bloqueadores de anuncios en el navegador y desactivar cualquier complemento innecesario del mismo. Asimismo, los expertos de la compañía aconsejan utilizar un antivirus y mantenerlo siempre actualizado, al igual que todo el software de todos los dispositivos.

Por otra parte, desde S2 Grupo advierten de la importancia de descargar solo software de las páginas oficiales y de estar siempre preparados y formados sobre los riesgos y las señales de advertencia del malvertising, así como conocer las prácticas de navegación segura.

"Tenemos que saber que igual que la IA se está utilizando con fines ilícitos, de la misma forma se está aplicando a la seguridad digital para detectar rápidamente anuncios potencialmente peligrosos y bloquearlos antes de que lleguen a los usuarios. En cualquier caso, la concienciación y la formación

sobre esta situación siempre será un paso fundamental para la ciberprotección", ha concluido José Rosell.

Datos de contacto:
Luis Núñez Canal
S2 Grupo
667574131

Nota de prensa publicada en: Madrid

Categorías: Nacional Inteligencia Artificial y Robótica Marketing Programación Software Ciberseguridad