Publicado en Madrid el 09/06/2023

Las tres amenazas deepfake más peligrosas de 2023

El número de deepfake o vídeos falsos crece a un ritmo anual del 900%, según el Foro Económico Mundial (WEF). Son casos que ocupan muchos titulares en los medios de comunicación y en los que el objetivo de los ciberdelincuentes es acosar, vengarse, realizar estafas… Ahora, los analistas de Kaspersky arrojan luz sobre los tres principales tipos de fraude basados en deepfake

El uso de redes neuronales (método de Inteligencia Artificial) y del aprendizaje profundo o Deep Learning (de ahí el término 'deepfake') permite prácticamente a cualquiera usar imágenes, vídeos y audio para crear vídeos realistas de alguien en los que se ha alterado digitalmente su rostro o su cuerpo para que parezca ser otra persona. El objetivo es difundir información falsa o maliciosa, así como realizar estafas.

Fraude financiero

Muchas veces, los ciberdelincuentes utilizan los deepfakes para hacerse pasar por famosos y que las víctimas caigan más fácilmente en el engaño. Un ejemplo de ello es un vídeo creado artificialmente el año pasado con Elon Musk como protagonista. En el mismo, el fundador de Tesla prometía grandes ganancias si se seguían una serie de consejos para invertir en criptomonedas. El contenido se volvió viral y muchos usuarios perdieron su dinero. Para crear deepfakes como este, los estafadores utilizan imágenes de celebrities o mezclan vídeos antiguos y lanzan transmisiones en directo en las redes sociales, prometiendo duplicar cualquier pago en criptomoneda que se les envíe.

Deepfakes pornográficos

Con la foto de una persona se puede crear una pieza pornográfica en la que aparezca manteniendo relaciones sexuales. En varias ocasiones han aparecido vídeos de este tipo utilizando rostros conocidos, pero las víctimas también pueden ser personas anónimas. Como consecuencia, las víctimas del ataque ven dañada su reputación y vulnerados sus derechos. Uno lo de los últimos ejemplos ha sido el de la cantante Rosalía, quien fue víctima de una foto falsificada donde aparecía, supuestamente, haciendo toples.

Riesgo para las empresas

Los deepfakes pueden utilizarse para atacar a empresas mediante extorsión, chantaje o espionaje industrial. En una ocasión, los ciberdelincuentes engañaron al gerente de un banco de Emiratos Árabes Unidos con este método, robando 35 millones de dólares. A partir de una pequeña grabación de voz, crearon una locución con la que lograron engañar al responsable de la entidad. En otro caso, los estafadores trataron de embaucar a la mayor plataforma de criptomonedas del mundo, Binance. Generaron un deepfake de uno de sus directivos y lo utilizaron en una reunión online en la que hablaron en nombre del ejecutivo.

En general, entre los objetivos de estos estafadores destacan la desinformación y la manipulación de la opinión pública o el chantaje. Los responsables de recursos humanos ya están en alerta ante el uso de deepfakes por parte de candidatos que solicitan trabajo a distancia, según una advertencia del FBI. En el caso de Binance, los atacantes utilizaron imágenes de personas que encontraron en Internet

para crear deepfakes para añadirlas a los currículos. Si consiguen engañar a los responsables de recursos humanos y más tarde reciben una oferta, pueden robar datos de la empresa.

¿Cómo elaboran los deepfakes?
Cuando los ciberdelincuentes preparan un deepfake, buscan muchos datos: fotos, vídeos, audio de la persona a suplantar. Los diferentes ángulos de cámara, la iluminación, las expresiones faciales… Todo supone un papel importante si se busca calidad. Se necesita también un ordenador y un software actualizados, puestos al día. Se trata de recursos al alcance de pocos ciberdelincuentes. Por ello, a pesar del peligro que implican, los deepfakes son una amenaza poco común, sobre todo si se tiene en cuenta que el precio por minuto de un vídeo falso puede alcanzar los 20.000 dólares si se trata de una creación de alta calidad.

"Uno de los grandes peligros de los deepfake para las empresas no es solo el robo de datos. Los riesgos reputacionales pueden tener consecuencias muy graves. Basta con imaginar la publicación de un vídeo en el que un ejecutivo (aparentemente) hace declaraciones sesgadas de temas delicados. Esto puede provocar la caída en bolsa de la compañía. Sin embargo, la posibilidad de que se produzcan estos ataques es extremadamente baja por el alto coste de creación si se quiere generar un deepfake realista", explica Dmitry Anikin, experto sénior de seguridad de Kaspersky.

"Es importante estar al tanto de los detalles que hacen sospechar que un vídeo es falso y mantener siempre una actitud escéptica. También hay que asegurarse de que los empleados entiendan qué es el deepfake y cómo pueden reconocerlo: movimientos bruscos, cambios en el tono de la piel, parpadeos extraños o directamente falta de parpadeo…", añade.

La monitorización constante de la darknet proporciona a Kaspersky información muy valiosa sobre la industria del deepfake. Esto permite conocer las últimas tendencias y actividades de los ciberdelincuentes. La monitorización y análisis es crítica, dado que ayuda a mejorar la visión del mapa de amenazas, siempre en constante cambio. Kaspersky's Digital Footprint utiliza esa monitorización, aportando mucha información y soluciones cuando se trata de amenazas relacionadas con los deepfakes.

Para protegerse de este tipo de engaño, Kaspersky recomienda:

- Revisar las prácticas de seguridad en la empresa, tanto en el apartado de software como en el de capacitación del personal y utilizar soluciones como Kaspersky Threat Intelligence para estar al corriente de las últimas amenazas.
- Crear un ‘muro humano’ informando al empleado sobre lo que es un deepfake y los riesgos que implica. Kaspersky Automated Security Awareness Platform mantiene a la plantilla informada sobre las últimas amenazas al tiempo que aumenta la alfabetización digital.
- Usar fuentes de información fiables. El desconocimiento informativo es clave para la proliferación de los deepfakes.
- Ser escéptico frente a videos o grabaciones de voz es importante. Ayuda a reducir las probabilidades de caer en la estafa.

Tener en cuenta las características que puedan indicar que un vídeo es falso, como movimientos bruscos, cambios en la iluminación y en el tono de la piel, parpadeo extraño o falta del mismo, labios mal sincronizados respecto a la voz o baja calidad de la reproducción.

Para aprender más sobre la industria del deepfake, visitar Kaspersky Daily.

Datos de contacto:
Mónica Iglesias
690196537

Nota de prensa publicada en: Madrid

Categorías: Nacional Inteligencia Artificial y Robótica Ciberseguridad Innovación Tecnológica