LITORALPRESS

Fecha: 11-09-2024
Medio: Diario Financiero
Supl. : Diario Financiero
Tipo: Noticia general
Título: "Ya existen muchas herramientas en el mercado negro para crear ataques con deepfake"

Pág. : 32
Cm2: 699,3

Tiraje: 16.150
Lectoría: 48.450
Favorabilidad: No Definida

María Isabel Manjarrez, investigadora senior de Seguridad del Equipo Global de Investigación y Análisis de Kaspersky.

"Ya existen muchas herramientas en el mercado negro para crear ataques con deepfake"

La experta de Kaspersky, alertó que la creación de imágenes falsas con IA generativa y la clonación de voces están afectando a Latinoamérica, y advirtió que la biometría facial "no es infalible" y que hay que tener siempre una doble autenticación.

POR ALEJANDRA RIVERA

Tal vez en alguna oportunidad una foto o un video generado con Inteligencia Artificial (IA) generativa lo hizo dudar de su autenticidad, tal vez no. Lo cierto es que las nuevas técnicas de *deepfake* (imagen falsa) y de clonación de voz no solo se están usando para poblar las redes sociales, sino también, para generar ataques cada vez más sofisticados a personas y empresas.

La investigadora *senior* de Seguridad del Equipo Global de Investigación y Análisis de Kaspersky, María Isabel Manjarrez, señaló a **DF**, en el marco de la Cyber Security Week que realizó la compañía global de ciberseguridad en agosto pasado, que desde la irrupción de la IA generativa, con ChatGPT como uno de sus principales exponentes, se ha visto un aumento de los ciberataques en Latinoamérica, los que usan técnicas como *deepfake* y clonación de voces.

La ingeniera en Telecomunicaciones y Sistemas Electrónicos del Instituto Tecnológico y de Estudios Superiores de Monterrey y responsable de investigar a los actores de amenaza más activos, seguir sus movimientos y analizar las nuevas técnicas implementadas, comentó que en la región se están detectando técnicas de ingeniería social, como el *phishing* (suplantación de identidad) para engañar a las personas, lo que seguirán en aumento.

"Ya existen muchas herramientas en el mercado negro para crear ataques con *deepfake*, incluso abiertas, es decir, de libre acceso, pero también hay otras de pago y aquí el punto es la calidad y es costo beneficio. Entre mejor calidad también es más caro el servicio", advirtió.

También comentó que es "muy difícil tener estadísticas de la *dark web*, donde se comercializan estas herramientas, pero alertó que hay muchos foros en canales clandestinos y en aplicaciones de mensajería donde se promocionan y distribuyen herramientas para crear ciberataques con IA generativa.

"Estos proveedores incluso, muestran las capacidades de sus herramientas, como el de Gringo 171, y las presumen, dan mucha información, hasta entregan consejos de dónde sacar datos, de cómo hacer contenido más realista", comentó.

– ¿Qué tipo de ataques, a través de deepfake o clonación de voz, están afectando a la región?

– El número de *deepfake* crece un 900% anual, según el Foro Económico Mundial. Los tres que más se ven en la región son el fraude financiero, empresarial y pornográfico.

Financiero, ya sea este tipo de transferencias suplantando una identidad o suplantando una voz. Pornográfico, en donde la víctima es puesta en una situación comprometedora, lo que puede llevar a chantajes, incluso empresarial. Ahí es en donde se juntan los tres, cuando se chantajea a un empleado para que comparta datos de la compañía. Y la empresarial, además del financiero, nos puede llevar al ciberespionaje inclusive, de información confidencial.

– ¿Cuáles son los sectores más impactados por estas nuevas amenazas?

– En la región, principalmente el financiero es el más afectado por la autenticación biométrica, muchas aplicaciones que las utilizan son las más impactadas, particularmente las de biometría facial, sobre todo por los *deepfake*.

También se usa mucho la huella digital, con la que desbloqueamos el teléfono y muchas aplicaciones de servicios como las bancarias.

– ¿La biometría facial dejó de ser un medio de autenticación válido en este nuevo contexto?

– La biometría en general no es infalible y no por ser facial es infalible.

Siempre hay que tener una doble autenticación, un doble factor, una contraseña para poder validar en primer lugar, que seamos nosotros, y en segundo lugar, que estemos tratando con un humano perfecto.

– ¿De qué países vienen las amenazas con IA generativa que afectan a Latinoamérica?

– Ahí es muy difícil saberlo, porque justamente están en canales clandestinos y utilizan identidades falsas para para crearlos. Pero hemos visto mucho *malware* (*software* malicioso) brasileño y mucho mercado (negro) en Brasil y también en la región, porque a los delincuentes le gusta mucho utilizar cosas en su idioma, lo que facilita el uso de las herramientas.

Regulación y educación

– ¿Qué se necesita para frenar este tipo de ciberataques a nivel de empresas? ¿Más inversión o regulación? ¿Ambas?

– Ambas. La tecnología avanza más rápido que las regulaciones y esto tiene que ir a la par y en el contexto de la región. No es la misma regulación que se necesita en Latinoamérica que en Europa o Asia. Y educación, por supuesto, tanto a nivel de usuarios como de áreas de tecnologías de la información, y de las personas, en general.

– Chile tiene una Ley Marco de Ciberseguridad recién estrenada, por ejemplo. ¿Marca alguna diferencia?

– Chile es puntero en Latinoamérica. Una ley de ciberseguridad, para empezar, pero también se requieren otras específicas de la tecnología, en el uso de inteligencia artificial va mucho de procesamiento de datos, porque se usa una cantidad de información impresionante, pero también en el uso ético de la tecnología para poner atención en estos datos que estamos usando.*