LITORALPRESS

Fecha: 09-07-2025
Medio: El Mercurio
Supl. : El Mercurio - Cuerpo A
Tipo: Noticia general
Título: **Impostor que usó IA para suplantar a secretario de Estado provoca alerta de seguridad en EE.UU.**

Pág. : 4
Cm2: 749,9

Tiraje: 126.654
Lectoría: 320.543
Favorabilidad: No Definida

Posible uso de *deepfake* en operaciones de espionaje:

Impostor que usó IA para suplantar a secretario de Estado provoca alerta de seguridad en EE.UU.

Utilizó mensajes de audio y texto que imitaban la voz y el estilo de escritura de Marco Rubio para contactar a funcionarios.

JEAN PALOU EGOAGUIRRE

El espionaje en la era de la inteligencia artificial ha dado una muestra más de sus posibilidades y riesgos, luego de que la Casa Blanca advirtiera de una operación de suplantación de identidad con tecnología de IA, que involucró al secretario de Estado estadounidense, Marco Rubio, y que aparentemente intentó acceder a información sensible.

El departamento de Estado alertó a sus diplomáticos en un cable enviado a todas las embajadas y consulados —al que accedió The Washington Post—, que un impostor no identificado utilizó *software* potenciado por IA para suplantar a Rubio en comunicaciones en las que utilizaba mensajes de voz y texto que imitaban su voz y estilo de escritura.

Según el cable diplomático, el actor malicioso que se hizo pasar por Rubio utilizó mensajes de texto y la aplicación de mensajería Signal —que la administración de Donald Trump emplea ampliamente— y logró "contactar a cinco personas ajenas al departamento, incluidos tres ministros de Relaciones Exteriores, un gobernador estadounidense y un miembro del Congreso", a los que no identifica. El documento afirma que el suplantador intentaba manipular a los funcionarios, "con el objetivo de obtener acceso a información o cuentas".

Acceso desde cuenta falsa de correo

La campaña comenzó en junio, cuando el impostor creó una cuenta en Signal con el nombre de usuario "Marco.Rubio@state.gov", que no corresponde a su dirección de correo real.

"No hay una amenaza cibernética directa para el departamento por esta campaña, pero la información compartida con un tercero podría ser expuesta si los individuos son comprometidos", asegura el cable del departamento de Estado, que dijo que está "investigando" y no entregó más detalles "por razones de seguridad".

FRANCE PRESSE

EL SECRETARIO DE ESTADO, Marco Rubio, ayer durante la reunión de gabinete del Presidente Donald Trump.

No es la primera vez que Rubio es suplantado en un "*deepfake*", como se conoce al tipo de contenido falso generado con IA que puede alterar imágenes, videos o audios. Hace unos meses, circuló un video falso del secretario de Estado, en el que decía que quería cortar el acceso de Ucrania al servicio de internet Starlink de Elon Musk, lo que fue desmentido.

El FBI ha venido advirtiendo que desde abril "actores maliciosos" se han hecho pasar por altos funcionarios, a través de mensajes de texto y de voz generados por IA, técnicas conocidas como *smishing* y *vishing*, respectivamente, "en un esfuerzo por establecer contacto antes de obtener acceso a cuentas personales". En mayo ocurrió un caso similar, cuando un suplantador se infiltró en el teléfono de la jefa de personal de la Casa Blanca, Susie Wiles, y envió mensajes y realizó llamadas en su nombre a senadores, gobernadores y empresarios que estaban en su agenda.

Un realismo cada vez mayor

Ya sea en estafas o en espionaje, la táctica de la suplantación de identidad tiene muchos años, pero ha dado un salto cualitativo últimamente con el lanzamiento de plataformas de IA —desarrolladas por empresas como Descript, Respeecher, Murf AI y iSpeech— que utilizan redes neuronales profundas para crear audios de alta calidad a partir de grabaciones, que generan voces que replican con precisión el tono, acento y estilo de habla de una persona.

"Es extremadamente fácil utilizar tanto *software* propietario como de código abierto para falsificar la voz de una persona a partir de una muestra de menos de un minuto. Estas técnicas se están utilizando ampliamente para estafar a personas en fraudes financieros. Y las mismas consideraciones aplican para la seguridad nacional que para la seguridad empresarial o individual frente al fraude: verificar la fuente de una solicitud y devolver la llamada a un número conocido para confirmar si la solicitud desde un número nuevo o un dispositivo desconocido proviene realmente de esa persona", dice a este diario el reconocido tecnólogo Sam Gregory, director ejecutivo de Witness.

NUEVAS TÁCTICAS

El FBI advirtió sobre el uso de las tácticas de *smishing* y *vishing* para suplantar identidades con herramientas de IA.

"Esta higiene digital básica reducirá la probabilidad de que las personas —incluidas aquellas en el poder— se confundan. Hemos visto que el audio es uno de los formatos de inteligencia artificial más utilizados para el engaño, precisamente porque es muy fácil de crear y difícil de detectar con el oído humano. Sin embargo, también está claro que la dirección del progreso tecnológico apunta hacia un realismo cada vez mayor y una producción más sencilla —de audio, pero también de video y video en vivo—, por lo que cada vez será más fácil suplantar identidades", advierte Gregory.

Los expertos recuerdan que no es la primera brecha de seguridad que muestra el gobierno de Trump en sus comunicaciones. En marzo, el entonces asesor de seguridad nacional de la Casa Blanca, Michael Waltz, agregó por error a un periodista a un grupo de Signal, donde se discutían planes de ataque altamente sensibles en Yemen, incidente que contribuyó a su salida del cargo y a reducir el uso de la aplicación para reuniones de seguridad nacional. Sin embargo, a nivel individual muchos funcionarios continúan usando esa *app* debido a su confiable cifrado de extremo a extremo.

Canales no oficiales

"Los estafadores han estado utilizando herramientas de IA para clonar voces y videos desde hace más de un año. Lo nuevo en el caso de Rubio es que los funcionarios del gobierno de Trump parecen usar canales no oficiales más que equipos anteriores de seguridad nacional", dice Jacob Shapiro, profesor de la Universidad de Princeton y experto en operaciones de *deepfake*. "La IA puede difuminar la línea entre lo real y lo falso, pero eso no debería importar mucho si los líderes se apegan a los canales oficiales de comunicación", remarca.

Jen Weedon, experta en seguridad informática de la Universidad de Columbia, explica que las herramientas de IA "reducen la barrera para la suplantación efectiva, permitiendo que actores maliciosos escalen sus esfuerzos y lleguen a personas de alto valor a través de los canales que utilizan, como en este caso Signal".

"Cuando la suplantación es de una figura política y los objetivos son otras figuras políticas, el espionaje es sin duda una posibilidad. Pero este tipo de obtención de información mediante comunicaciones digitales ocurre desde hace tiempo; la IA generativa solo lo hace más fácil y rápido", plantea Weedon. "Los gobiernos deberían seguir adoptando y haciendo cumplir protocolos más estrictos de verificación en las comunicaciones digitales, como la autenticación multifactor, la verificación criptográfica de identidad y el uso de canales seguros con validación humana, para contrarrestar la suplantación impulsada por IA y otras filtraciones. También son fundamentales las capacitaciones periódicas sobre ingeniería social habilitada por IA y un mayor control del uso de tecnología en dispositivos móviles, incluyendo no usar aplicaciones comerciales comunes para comunicar información sensible en chats grupales".