

Un estudio determinó que la inteligencia artificial puede descifrar contraseñas a partir del ruido de las teclas

12/08/2023



El ruido del teclado al ingresar contraseñas podría abrir la puerta a ciberataques, según un estudio reciente. La **Universidad de Surrey** encontró que la **inteligencia artificial** puede descifrar claves basándose en los sonidos de las teclas al ser pulsadas.

En un nuevo informe de investigación, expertos de la **Universidad de Surrey** revelaron que la **inteligencia artificial** es capaz de interpretar los sonidos de las teclas para descifrar contraseñas. Mediante la grabación de las pulsaciones y la formación de un modelo de «*deep learning*», tres investigadores lograron más del **90%** de

precisión en la interpretación de los sonidos del teclado.

Los resultados indicaron que **el uso de herramientas de videoconferencia como Zoom y dispositivos con micrófonos incorporados podría aumentar las amenazas de ciberataques**, los cuales estarían basados en los sonidos capturados previamente.

✘ **Los sonidos de las teclas podrían ser un elemento a tener en cuenta por los hackers. Foto: NA.**

En su artículo titulado *«Un práctico ataque acústico de canal lateral en teclados basado en aprendizaje profundo»*, los investigadores **Joshua Harrison, Ehsan Toreini y Marhyam Mehrnezhad** advirtieron que las tecnologías de aprendizaje, las computadoras portátiles actuales y la utilización de videollamadas representan una seria amenaza de ciberseguridad.

Los expertos desarrollaron un sistema mediante **algoritmos de aprendizaje automático** para identificar las teclas presionadas en una computadora a través del sonido mecánico que generan. Mediante la **grabación de dichos sonidos** mientras pulsaban las teclas de una MacBook Pro en diferentes formas, **el equipo entrenó un sistema que pudo identificar las teclas correctas** en un 95% de las veces durante llamadas telefónicas y un 93% durante videollamadas por Zoom. ✘

Te puede interesar:

Crece la tensión: Joe Biden limita inversiones estadounidenses en China en tecnología e inteligencia artificial

Cómo prevenir un ataque

A pesar de que no se utilizaron estos métodos para descifrar contraseñas, los investigadores enfatizaron en la importancia de la **precaución de los usuarios**. Con el fin evitar posibles riesgos de seguridad o robo de datos, recomendaron optar por **contraseñas biométricas y activar la autenticación en dos**

pasos cada vez que se pueda.

✘ El resultado preliminar de la investigación arrojó que se identificaron más rápido las teclas que se ubican cerca del borde de la computadora. Foto: Reuters.

En su defecto, es recomendable **crear una contraseña que contenga una mezcla de mayúsculas y minúsculas, o de números y símbolos.** De esta forma, será mucho más difícil para los hackers averiguar cuándo alguien activa o desactiva la tecla de Bloq Mayús.

Fuente: Canal 26