Una investigación reveló que una técnica de ataque de hace tres años para eludir el audio de reCAPTCHA de Google mediante el uso de su propia API Speech-to-Text, aún funciona con un 97% de precisión.

El investigador Nikolai Tschacher reveló sus hallazgos en una prueba de concepto (PoC) del ataque el pasado 2 de enero de 2021.

> *«La idea del ataque es muy simple: agarras el archivo MP3 del audio reCAPTCHA y lo envías a la API de voz a texto de Google. Google devolverá la respuesta correcta en más del 97% de todos los casos»*, dijo Tschacher.

Introducido en 2014, CAPTCHA (o prueba de Turing pública completamente automatizada para diferenciar a las computadoras y los humanos) es un tipo de prueba de desafío-respuesta diseñada para proteger contra la creación automatizada de cuentas y el abuso del servicio al presentar a los usuarios una pregunta que es fácil de resolver para los humanos, pero difícil para las computadoras.

reCAPTCHA es una versión más reciente de la tecnología CAPTCHA que fue adquirida por Google en 2009. La compañía lanzó la tercera versión de reCAPTCHA en octubre de 2018. Elimina completamente la necesidad de interrumpir a los usuarios con desafíos a favor de una puntuación (o a 1) que se devuelve en función del comportamiento de un visitante en el sitio web, todo sin la interacción del usuario.

Todo el ataque depende de una investigación denominada unCaptcha, publicada por investigadores de la Universidad de Maryland en abril de 2017, dirigida a la versión de audio de reCAPTCHA. Ofrecido por razones de accesibilidad, plantea un desafío de audio, ya que permite a las personas con pérdida de visión reproducir o descargar la muestra de audio y resolver la pregunta.

Para llevar a cabo el ataque, la carga útil de audio se identifica mediante la programación en la página utilizando herramientas como Selenium, luego se descarga y se alimenta a un

servicio de transcripción de audio en línea como Google Speech-to-Text API, cuyos resultados se utilizan en última instancia para burlar el audio del CAPTCHA.

Luego de la divulgación del ataque, Google actualizó reCAPTCHA en junio de 2018 con una mejor detección de bots y soporte para frases habladas en lugar de dígitos, pero no lo suficiente para frustrar el ataque, ya que los investigadores lanzaron unCaptcha2 como PoC con una precisión aún mayor, del 91%, en comparación con el 85% de UnCaptcha, mediante el uso de un *«clicker de pantalla para moverse a ciertos píxeles en la pantalla y moverse por la página como un humano».*

El esfuerzo de Tschacher es un intento de mantener el PoC actualizado y en funcionamiento, haciendo posible eludir la versión de audio de reCAPTCHA v2.

> *«Aún peor: reCAPTCHA v2 todavía se usa en el nuevo reCAPTCHA v3 como un mecanismo de respaldo»,* dijo Tschacher.

Con reCAPTCHA utilizado por cientos de miles de sitios para detectar tráfico abusivo y creación de cuentas de bots, el ataque es un recordatorio de que no siempre es infalible y de las importantes consecuencias que puede tener un desvío.

En marzo de 2018, Google abordó una falla separada en reCAPTCHA que permitió que una aplicación web que usaba la tecnología creara una solicitud a *«/recaptcha/api/siteverify»* de forma insegura y evitara la protección en todo momento.