09/07/2023

NUIT: la nueva herramienta de los ciberdelincuentes para hackear nuestros dispositivos a través de ondas sonoras

Un equipo de investigadores de la Universidad de Texas, en colaboración con la Universidad de Colorado, han desarrollado una nueva técnica para transmitir en secreto órdenes dañinas a nuestros terminales

Si pensaba que los ciberdelincuentes ya contaban con suficientes herramientas maliciosas para intentar infectar nuestros terminales, se equivocaba. Según un nuevo estudio, un equipo de investigadores de la Universidad de Texas en San Antonio, en colaboración con la Universidad de Colorado, han desarrollado una **nueva técnica para transmitir en secreto órdenes dañinas a nuestros dispositivos** electrónicos, a través de **ondas de sonido**. Llamado 'troyano inaudible de ultrasonido cercano' (NUIT, por sus siglas en inglés), esta nueva herramienta puede lanzar ataques silenciosos contra dispositivos que utilizan asistentes de voz, como teléfonos inteligentes, altavoces inteligentes y otras IoT (Internet de las cosas), la tecnología que facilita la comunicación entre los dispositivos y la nube, así como entre otros dispositivos.

En una serie de videos publicados en Youtube, los investigadores demostraron cómo realizaron estos ataques en una variedad de dispositivos, incluidos teléfonos inteligentes, iOS y Android, altavoces inteligentes, Google Home y Amazon Echo, y Windows Cortana.

Los investigadores revelaron que los ataques NUIT se pueden realizar utilizando dos métodos diferentes:

- El primer método, NUIT-1, es cuando un dispositivo es tanto el origen como el objetivo del ataque. Por ejemplo, se puede lanzar un ataque en un teléfono inteligente al reproducir un archivo de audio que hace que el dispositivo realice una acción, como abrir la puerta de un garaje o enviar un mensaje de texto.
- El otro método, NUIT-2, es cuando el ataque lo lanza un dispositivo con altavoz a otro dispositivo con micrófono, como un sitio web a un altavoz inteligente.

«Si reproduce YouTube en su televisor inteligente, ese televisor inteligente tiene un altavoz, ¿verdad? El sonido de los comandos maliciosos de NUIT se volverá inaudible y también puede atacar su teléfono celular y comunicarse con su Asistente de Google o dispositivos Alexa», explicó Guenevere Chen, una de los autoras de la investigación, a lo que añadió: «Incluso puede suceder durante una reunión de Zoom. Si alguien activa el sonido, puede incorporar la señal de ataque para piratear su teléfono que se encuentra junto a su ordenador durante la reunión».

Condiciones para realizar los ataques

Asimismo, Chen explicó que el altavoz desde donde se lanza el NUIT **debe configurarse por encima de un cierto nivel de volumen y que los comandos maliciosos duren solo 0,77 segundos** para que funcione el ataque. No obstante, en la mayoría de los casos, **la 'voz' inaudible ni siquiera necesita ser reconocida por el terminal como el usuario autorizado** , reveló. «De los 17 dispositivos inteligentes que probamos, a los dispositivos Apple Siri necesitan robar la voz del usuario, mientras que otros dispositivos de asistente de voz pueden activarse usando cualquier voz o la voz de un robot». Revelando a su vez que es menos probable que los dispositivos que están conectados a auriculares sean vulnerables a ser utilizados por un atacante. «Si no usa el altavoz para transmitir sonido, es menos probable que sea atacado por NUIT», expresó Chen, a lo que añadió: «El uso de

auriculares establece una limitación en la que el sonido de los auriculares es demasiado bajo para transmitirlo al micrófono. Si el micrófono no puede recibir el comando malicioso inaudible, la NUIT no puede activar maliciosamente el asistente de voz subyacente».

Fuente: abc.es

LINK DE LA NOTICIA