Un equipo de investigadores de seguridad cibernética desarrolló y demostró una nueva técnica de ataque de canal lateral, que puede aplicarse por espías para recuperar el sonido completo de la habitación de la víctima que contiene una bombilla suspendida.

Los hallazgos fueron publicados en un nuevo artículo por un equipo de académicos: Ben Nassi, Yaron Pirutin, Adi Shamir, Yuval Elovici y Boris Zadov, de la Universidad israelí Ben-Gurion del Negev y el Instituto de Ciencias Weizmann, que también será presentado en el Black Hat USA 2020 a finales de agosto.

La técnica de espionaje a larga distancia, denominada «*Lamphone*«, funciona al capturar ondas de sonido minúsculas por medio de un sensor electro-óptico a la bombilla y utilizándola para recuperar el habla y reconocer la música.

Funcionamiento del ataque Lamphone

Para que Lamphone suceda con éxito, es necesario detectar las vibraciones de las bombillas colgantes como resultado de las fluctuaciones de la presión del aire que ocurren de forma natural cuando las ondas de sonido golpean sus superficies, y medir los pequeños cambios en la salida de la bombilla que esas pequeñas vibraciones activan para recoger fragmentos de conversaciones e identificar música.

> *«Asumimos una víctima ubicada dentro de una habitación que contiene una bombilla colgante. Consideramos que un espía es una entidad maliciosa que está interesada en espiar a la víctima para capturar las conversaciones de la víctima y hacer uso de la información proporcionada en la conversación (por ejemplo, robar el número de tarjeta de crédito de la víctima, realizar una extorsión basada en información privada revelada por la víctima, etc.)»,* dijeron los investigadores.

Para lograr esto, la configuración consiste en un telescopio para proporcionar una vista de

primer plano de la habitación que contiene la bombilla desde la distancia, un sensor electro-óptico que está montado en el telescopio para convertir la luz en una corriente eléctrica, una señal analógica a convertidor digital para transformar la salida del sensor en una señal digital, y una computadora portátil para procesar las señales ópticas entrantes y emitir los datos de sonido recuperados.

> *«Lamphone aprovecha las ventajas de los métodos de micrófono visual (pasivo) y micrófono láser (se puede aplicar en tiempo real) para recuperar el habla y el sonido»,* dijeron los investigadores.

Demostración

Los investigadores recuperaron un extracto audible del discurso del presidente Donald Trump, que podría ser transcrito por la API de voz a texto de Google. También reprodujeron una grabación de «Let it Be» de The Beatles y «Clocks» de Coldplay, que fueron lo suficientemente claros para ser reconocidos por los servicios de identificación de canciones como Shazam y SoundHound.

> *«Mostramos cómo las fluctuaciones en la presión del aire en la superficie de la bombilla colgante, que hacen que la bombilla vibre ligeramente, pueden ser explotadas por los espías para recuperar el habla y el canto, pasivamente, externamente y en tiempo real»,* agregaron los investigadores.

> *«Analizamos la respuesta de una bombilla colgante al sonido por medio de un sensor electro-óptico y aprendemos cómo aislar la señal de audio de la señal óptica. Con base en nuestro análisis, desarrollamos un algoritmo para recuperar el sonido de las mediciones ópticas obtenidas de las vibraciones de una bombilla y capturada por el sensor electro-óptico»,* agregaron.

El enfoque del ataque es efectivo desde grandes distancias, comenzando por al menos 25 metros de distancia del objetivo, utilizando un telescopio y un sensor electro-óptico de 400 dólares, y puede amplificarse aún más con equipos de alto rango.

Los ataques de canal lateral de Lamphone se pueden aplicar en escenarios en tiempo real, a diferencia de las configuraciones de espionaje anteriores, como Visual Microphone, que se ven obstaculizadas por largos períodos de procesamiento para recuperar unos segundos de discurso.

Además, debido a que es un escenario completamente externo, el ataque no requiere que un actor malicioso comprometa el dispositivo de ninguna víctima.

Debido a que la efectividad del ataque depende mucho de la salida de la luz, las medidas para mitigar o evitar el ataque propuestas por los investigadores, podrían ser la reducción de la cantidad de luz capturada por el sensor electro-óptico mediante el uso de una bombilla más débil y un muro cortina para limitar la luz emitida desde una habitación.

Además, podría usarse una bombilla más pesada para minimizar las vibraciones causadas por los cambios en la presión del aire.