Un nuevo tipo de ataque de canal lateral conocido como PIXHELL podría usarse para atacar computadoras aisladas al superar la *«brecha de audio»* y extraer información sensible aprovechando el ruido generado por los píxeles en la pantalla.

> *«El malware en computadoras con brechas de aire y audio crea patrones de píxeles diseñados que generan ruido en el rango de frecuencia de 0 a 22 kHz»*, explicó el Dr. Mordechai Guri, director del Laboratorio de Investigación en Ciberseguridad Ofensiva en el Departamento de Ingeniería de Software y Sistemas de Información de la Universidad Ben Gurion del Negev en Israel, en un artículo recientemente publicado.
>
> *«El código malicioso aprovecha el sonido producido por bobinas y capacitores para controlar las frecuencias que emanan de la pantalla. Las señales acústicas pueden codificar y transmitir información confidencial.»*

Este ataque es relevante porque no requiere hardware de audio especializado, altavoces externos o altavoces internos en la computadora comprometida; en lugar de eso, utiliza la pantalla LCD para generar señales acústicas.

El aislamiento de aire (air-gapping) es una medida de seguridad fundamental diseñada para proteger entornos críticos contra posibles amenazas, aislándolos física y lógicamente de redes externas, como Internet. Esto se logra normalmente desconectando cables de red, desactivando interfaces inalámbricas y desconectando conexiones USB.

Sin embargo, estas medidas de seguridad pueden ser vulneradas por un infiltrado malicioso o un compromiso en la cadena de suministro de hardware o software. Otra posibilidad es que un empleado desprevenido conecte una unidad USB infectada para instalar malware capaz de establecer un canal encubierto de exfiltración de datos.

> *«Phishing, empleados maliciosos u otras técnicas de ingeniería social pueden ser utilizadas para engañar a personas con acceso al sistema aislado para que realicen acciones que pongan en riesgo la seguridad, como hacer clic en enlaces maliciosos o descargar archivos infectados»,* comentó el Dr. Guri.

> *«Los atacantes también pueden emplear ataques a la cadena de suministro de software al dirigirse a dependencias de aplicaciones o bibliotecas de terceros. Al comprometer estas dependencias, pueden introducir vulnerabilidades o código malicioso que podría no ser detectado durante el desarrollo y las pruebas.»*

Al igual que el ataque RAMBO recientemente revelado, PIXHELL utiliza el malware en el host comprometido para crear un canal acústico que filtra información de sistemas con brechas de audio.

Esto es posible porque las pantallas LCD contienen inductores y capacitores en sus componentes internos y en su fuente de alimentación, lo que provoca que vibren a una frecuencia audible, produciendo un ruido agudo cuando la electricidad pasa a través de las bobinas, un fenómeno conocido como «coil whine» o zumbido de bobina.

En particular, los cambios en el consumo de energía pueden inducir vibraciones mecánicas o efectos piezoeléctricos en los capacitores, generando ruido audible. Un aspecto importante que afecta el patrón de consumo es la cantidad de píxeles iluminados y su distribución en la pantalla, ya que los píxeles blancos requieren más energía para ser mostrados que los píxeles oscuros.

> *«Además, cuando la corriente alterna (CA) circula por los capacitores de la pantalla, estos vibran a frecuencias específicas. Las emisiones acústicas son generadas por la parte eléctrica interna de la pantalla LCD. Sus características están influenciadas por el mapa de bits, el patrón y la intensidad de los píxeles proyectados en la pantalla»*, explicó el Dr. Guri.

> *«Al controlar minuciosamente los patrones de píxeles en nuestra pantalla, nuestra técnica puede generar ondas acústicas a frecuencias específicas a partir de pantallas LCD.»*

De esta manera, un atacante podría utilizar esta técnica para extraer datos en forma de señales acústicas, que luego serían moduladas y enviadas a un dispositivo cercano con Windows o Android. Este dispositivo puede desmodular los paquetes y recuperar la información.

Sin embargo, es importante señalar que la potencia y calidad de la señal acústica emitida dependen de la estructura específica de la pantalla, su fuente de alimentación interna, y la ubicación de las bobinas y capacitores, entre otros factores.

Otro aspecto relevante es que el ataque PIXHELL, en su forma predeterminada, es visible para los usuarios que están mirando la pantalla LCD, ya que implica la visualización de un patrón de mapa de bits compuesto por filas alternas de blanco y negro.

> *«Para mantener el ataque encubierto, los atacantes podrían emplear una estrategia que permita la transmisión mientras el usuario no está presente. Por ejemplo, un 'ataque nocturno' en los canales encubiertos se lleva a cabo durante las horas en que el sistema está inactivo, lo que disminuye el riesgo de ser detectado y expuesto»,* comentó el Dr. Guri.

El ataque también puede convertirse en uno más sigiloso durante el horario laboral al reducir los colores de los píxeles a valores muy bajos antes de la transmisión —por ejemplo, usando niveles RGB de (1,1,1), (3,3,3), (7,7,7) y (15,15,15)—, lo que hace que la pantalla parezca negra para el usuario.

No obstante, esto provoca una *«reducción significativa»* en los niveles de producción de sonido. Además, esta estrategia no es infalible, ya que un usuario podría notar patrones

anómalos si observa la pantalla con *«atención»*.

Esta no es la primera vez que se superan las restricciones de brecha de audio en un entorno experimental. Investigaciones anteriores del Dr. Guri han utilizado sonidos generados por ventiladores de computadoras (Fansmitter), discos duros (Diskfiltration), unidades de CD/DVD (CD-LEAK), fuentes de alimentación (POWER-SUPPLaY), y impresoras de inyección de tinta (Inkfiltration).

Como medidas preventivas, se recomienda el uso de un bloqueador acústico para contrarrestar la transmisión, vigilar el espectro de audio en busca de señales inusuales, restringir el acceso físico a personal autorizado, prohibir el uso de teléfonos inteligentes, y emplear una cámara externa para identificar patrones modulares inusuales en la pantalla.