El investigador de seguridad cibernética Mordechai Guri, de la Universidad Ben Gurion del Negev de Israel, demostró recientemente un nuevo tipo de malware que podría usarse para robar de forma encubierta, datos altamente sensibles de sistemas con espacio de aire y audio utilizando una novedad acústica en unidades de fuente de alimentación que cuentan con dispositivos informáticos modernos.

Nombrado como POWER-SUPPLaY, la investigación se basa en una serie de técnicas que aprovechan canales encubiertos electromagnéticos, acústicos, térmicos, ópticos e incluso, cables de alimentación para filtrar datos de computadoras que no están en red.

> *«Nuestro malware desarrollado puede explotar la unidad de fuente de alimentación de la computadora (PSU) para reproducir sonidos y usarlo como un altavoz secundario fuera de banda con capacidades limitadas»,* dijo el Dr. Guri.
>
> *«El código malicioso manipula la frecuencia de conmutación interna de la fuente de alimentación y, por lo tanto, controla las formas de onda de sonido generadas por sus condensadores y transformadores. Mostramos que nuestra técnica funciona con distintos tipos de sistemas: estaciones de trabajo de PC y servidores, así como sistemas integrados y dispositivos IoT que no tienen hardware de audio. Los datos binarios pueden ser modulados y transmitidos por medio de las señales acústicas».*

Fuente de alimentación usada como altavoz fuera de banda

Los sistemas con espacio de aire se consideran una necesidad en entornos donde los datos confidenciales están involucrados en un intento por reducir el riesgo de fuga de datos. Los dispositivos suelen tener su hardware de audio deshabilitado para evitar que los adversarios aprovechen los altavoces y micrófonos incorporados para robar información por medio de ondas sónicas y ultrasónicas.

También requiere que tanto las máquinas transmisoras como las receptoras estén ubicadas muy cerca unas de otras y que estén infectadas con el malware adecuado para establecer el enlace de comunicación, por ejemplo, a través de campañas de ingeniería social que exploten las vulnerabilidades del dispositivo objetivo.

POWER-SUPPLaY funciona de la misma forma en que el malware se ejecuta en una PC, puede aprovechar su PSU y usarlo como un altavoz fuera de banda, evitando de este modo la necesidad de hardware de audio especializado.

> *«Esta técnica permite reproducir transmisores de audio desde una computadora incluso cuando el hardware de audio está desactivado y los altavoces no están presentes. Los datos binarios se pueden modular y transmitir por medio de las señales acústicas. Las señales acústicas pueden ser interceptadas por un receptor cercano, que demodula y decodifica los datos y los envía al atacante por medio de Internet»*, dijo el investigador.

En otras palabras, el malware de espacio de aire regula la carga de trabajo de las CPU modernas para controlar su consumo de energía y la frecuencia de conmutación de la PSU para emitir una señal acústica en el rango de 0-24 KHz y modular los datos binarios sobre ella.

Bypass de espacio de aire y seguimiento de dispositivos cruzados

El malware en la computadora comprometida no solo acumula datos confidenciales (archivos, URL, pulsaciones de teclas, claves de cifrado, etc), además, transmite datos en formato WAV utilizando las ondas de sonido acústicas emitidas por la fuente de alimentación de la computadora, que se decodifica por el receptor, en este caso, una aplicación que se ejecuta en un teléfono inteligente Android.

Según el investigador, un atacante puede extraer datos de sistemas con espacios de audio al teléfono cercano ubicado a 2.5 metros de distancia con una velocidad de bits máxima de 50 bits/seg.

Una consecuencia de este ataque que afecta la privacidad, es el rastreo entre dispositivos, ya que la técnica permite que el malware capture el historial de navegación en el sistema comprometido y transmita la información al receptor.

Como contramedida, el investigador sugiere sistemas sensibles a la zonificación en áreas restringidas donde los teléfonos móviles y otros equipos electrónicos están prohibidos. Tener un sistema de detección de intrusos para monitorear el comportamiento sospechoso de la CPU y configurar detectores de señales y bloqueadores basados en hardware también podría ayudar a defenderse contra el canal secreto propuesto.

Debido a que las instalaciones nucleares con espacios de aire en Irán e India son blanco de violaciones de seguridad, la nueva investigación es otro recordatorio de que los ataques complejos de la cadena de suministro pueden dirigirse contra sistemas aislados.

> *«El código POWER-SUPPLaY puede funcionar desde un proceso ordinario en modo de usuario y no necesita acceso a hardware o privilegios de root. Este método propuesto no invoca llamadas especiales del sistema ni accede a recursos de hardware, y por lo tanto es muy evasivo»*.