Se ha descubierto un nuevo ataque de canal lateral que utiliza las señales de radio emitidas por la memoria de acceso aleatorio (RAM) de un dispositivo como método para extraer datos, lo que supone un riesgo para las redes aisladas (air-gapped).

Esta técnica ha sido bautizada como RAMBO por el Dr. Mordechai Guri, director del Laboratorio de Investigación Cibernética Ofensiva del Departamento de Ingeniería de Sistemas de Información y Software de la Universidad Ben Gurion del Negev, en Israel.

> *«Mediante señales de radio generadas por software, un malware puede codificar información sensible, como archivos, imágenes, registros de pulsaciones de teclas, datos biométricos o claves de cifrado»,* señaló el Dr. Guri en un artículo de investigación reciente.
>
> *«Con hardware de radio definido por software (SDR) y una antena comercial sencilla, un atacante puede interceptar las señales de radio emitidas desde cierta distancia. Estas señales luego pueden ser decodificadas y convertidas nuevamente en información binaria».*

A lo largo de su carrera, el Dr. Guri ha desarrollado varios métodos para extraer datos confidenciales de redes aisladas, utilizando cables Serial ATA (SATAn), giroscopios MEMS (GAIROSCOPE), luces LED de las tarjetas de red (ETHERLED) y variaciones en el consumo energético (COVID-bit).

Entre otras técnicas poco convencionales que ha ideado para filtrar datos de redes air-gapped se incluyen señales acústicas secretas generadas por los ventiladores de las tarjetas gráficas (GPU-FAN), ondas sonoras o ultrasónicas emitidas por los zumbadores de las placas base (EL-GRILLO), e incluso los paneles de las impresoras y sus luces LED (PrinterLeak).

El año pasado, Guri también mostró AirKeyLogger, un ataque de keylogging mediante

radiofrecuencia sin necesidad de hardware adicional, que aprovecha las emisiones de radiofrecuencia del suministro de energía de un equipo para extraer pulsaciones de teclas en tiempo real a un atacante remoto.

> *«Para filtrar datos confidenciales, las frecuencias de trabajo del procesador se manipulan, generando emisiones electromagnéticas desde la fuente de energía, moduladas por las pulsaciones de teclas. La información sobre las pulsaciones puede ser captada a varios metros de distancia usando un receptor de radiofrecuencia o un smartphone con una antena simple»,* explicó Guri en su estudio.

Como ocurre en este tipo de ataques, es necesario comprometer primero la red aislada mediante otros métodos, como la intervención de un infiltrado, el uso de memorias USB contaminadas o un ataque a la cadena de suministro. Una vez hecho esto, el malware activa el canal de exfiltración de datos oculto.

RAMBO sigue este patrón, ya que el malware manipula la RAM para generar señales de radio a frecuencias de reloj, que luego son codificadas usando codificación Manchester y transmitidas para ser captadas a distancia.

La información codificada puede incluir pulsaciones de teclas, documentos e información biométrica. El atacante, utilizando SDR, puede recibir estas señales electromagnéticas, demodularlas, decodificarlas y recuperar los datos exfiltrados.

> *«El malware aprovecha las emisiones electromagnéticas de la RAM para modular la información y transmitirla hacia el exterior. Un atacante remoto con un receptor de radio y una antena puede recibir los datos, demodularlos y decodificarlos en su formato binario o textual original»,* explicó el Dr. Guri.

Según el estudio, esta técnica podría emplearse para extraer datos de computadoras aisladas que utilicen CPUs Intel i7 de 3.6 GHz y 16 GB de RAM, a una velocidad de 1,000 bits por segundo, permitiendo exfiltrar pulsaciones de teclas en tiempo real a una tasa de 16 bits por tecla.

> *«Una clave de cifrado RSA de 4096 bits puede extraerse en 41.96 segundos a baja velocidad y en 4.096 segundos a alta velocidad. La información biométrica, los archivos pequeños (.jpg) y documentos pequeños (.txt y .docx) requieren 400 segundos a baja velocidad y solo unos segundos a velocidad alta»,* añadió el Dr. Guri.
>
> *«Esto sugiere que el canal encubierto RAMBO puede emplearse para filtrar información breve en un tiempo reducido».*

Las medidas de protección contra este ataque incluyen aplicar restricciones de zonas «rojo-negro» para la transferencia de información, utilizar sistemas de detección de intrusos (IDS), monitorizar el acceso a la memoria a nivel de hipervisor, emplear bloqueadores de radiofrecuencia para interferir las comunicaciones inalámbricas, y utilizar una jaula de Faraday.