Un mecanismo de exfiltración de datos recientemente descubierto emplea cables Ethernet como una *«antena de transmisión»* para desviar de forma sigilosa datos altamente sensibles en sistemas con espacios de aire, según las últimas investigaciones.

> *«Es interesante que los cables que vinieron a proteger el espacio de aire se conviertan en la vulnerabilidad del espacio de aire en este ataque»,* dijo el Dr. Mordechai Guri, jefe de I + D en el Centro de Investigación de Seguridad Cibernética de la Universidad Ben Gurion del Negev en Israel.

Apodada como *«LANtenna Attack»,* la novedosa técnica permite que el código malicioso en computadoras con espacio de aire acumule datos confidenciales y luego los codifique a través de ondas de radio que emanan de cables Ethernet como si fueran antenas. Las señales transmitidas pueden ser interceptadas después por un receptor de radio definido por software (SDR) cercano de forma inalámbrica, los datos decodificados y enviados a un atacante que se encuentra en una habitación adyacente.

«En particular, el código malicioso puede ejecutarse en un proceso de modo de usuario ordinario y funcionar con éxito desde dentro de una máquina virtual», dijeron los investigadores es un documento titulado *«LANTENNA: Extracción de datos de redes con espacio de aire a través de cables Ethernet».*

Las redes con espacios abiertos están diseñadas como una medida de seguridad de la red para minimizar el riesgo de fuga de información y otras amenazas cibernéticas al garantizar que una o más computadoras estén físicamente aisladas de otras redes, como Internet o una red de área local. Por lo general, están cableados ya que las máquinas que forman parte de dichas redes tienen sus interfaces de red inalámbrica desactivadas permanentemente o eliminadas físicamente.

Esta no es la primera vez que el Dr. Guri demuestra formas poco convencionales de filtrar datos confidenciales de computadoras con espacio de aire. En febrero de 2020, el investigador de seguridad ideó un método que emplea pequeños cambios en el brillo de la

pantalla LCD, que permanecen invisibles a simple vista, para modular la información binaria en patrones similares al código morse de forma encubierta.

Después, en mayo de 2020, el Dr. Guri demostró cómo el malware podía explotar la unidad de fuente de alimentación (PSU) de una computadora para reproducir sonidos y utilizarla como un altavoz secundario fuera de banda para filtrar datos en un ataque llamado *«POWER-SUPPLaY»*.

Por último, en diciembre de 2020, el investigador mostró *«AIR-FI»,* un ataque que aprovecha las señales de Wi-Fi como un canal encubierto para exfiltrar información confidencial sin siquiera requerir la presencia de hardware de WiFi dedicado en los sistemas objetivo.

El ataque LANtenna no es distinto en el funcionamiento de utilización de malware en la estación de trabajo con espacio de aire para inducir al cable Ethernet a generar emisiones electromagnéticas en las bandas de frecuencia de 125 MHz, que luego son moduladas e interceptadas por un receptor de radio cercano. En una demostración de prueba de concepto, los datos transmitidos desde una computadora con espacio de aire por medio de su cable Ethernet se recibieron a una distancia de 200 cm.

Al igual que otros ataques de fuga de datos de este tipo, la activación de la infección requiere la implementación del malware en la red de destino a través de cualquiera de los diferentes vectores de infección que van desde ataques a la cadena de suministro o unidades USB contaminadas hasta técnicas de ingeniería social, credenciales robadas o mediante el uso de iniciados maliciosos.

Como contramedidas, los investigadores proponen prohibir el uso de receptores de radio en y alrededor de redes con espacio de aire y monitorear la actividad de la capa de enlace de la tarjeta de interfaz de red para cualquier canal encubierto, así como bloquear las señales y usar blindaje metálico para limitar la interferencia de los campos electromagnéticos que se emana de los cables blindados.

> *«Este documento muestra que los atacantes pueden explotar los cables Ethernet para filtrar datos de redes con espacios de aire. El malware instalado en una estación de trabajo segura, computadora portátil o dispositivo integrado puede invocar varias actividades de red que generan emisiones electromagnéticas de los cables Ethernet»,* dijeron los investigadores.
>
> *«Las antenas dedicadas y costosas ofrecen una mejor distancia y podrían alcanzar decenas de metros con algunos cables»,* agregó el Dr. Guri.