Un nuevo método diseñado para filtrar información y saltar por encima de los espacios de aire aprovecha los cables Serial Advanced Technology Attachment (SATA) o Serial ATA como medio de comunicación, lo que se suma a una larga lista de métodos electromagnéticos, magnéticos, eléctricos, ópticos y acústicos que ya existen y se ha demostrado su uso para robar datos.

> *«Aunque las computadoras con espacio de aire no tienen conectividad inalámbrica, mostramos que los atacantes pueden usar el cable SATA como una antena inalámbrica para transferir señales de radio en la banda de frecuencia de 6 GHz»*, 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.

La técnica, denominada SATAn, se aprovecha de la prevalencia de la interfaz del bus de la computadora, lo que la hace *«altamente disponible para los atacantes en una amplia gama de sistemas informáticos y entornos de TI».*

En pocas palabras, el objetivo es utilizar el cable SATA como un canal encubierto para emanar señales electromagnéticas y transferir una breve cantidad de información confidencial de computadoras altamente seguras y con espacio de aire de forma inalámbrica a un receptor cercano a más de 1 metro de distancia.

Una red con espacio de aire es aquella que está físicamente aislada de cualquier otra red para aumentar su seguridad. El airgapping se considera un mecanismo esencial para salvaguardar sistemas de alto valor que son de gran interés para los actores de amenazas motivados por el espionaje.

Los ataques dirigidos a sistemas críticos de control de misiones han crecido en número y sofisticación en los últimos años, como se observó recientemente en el caso de Industroyer 2 y PIPEDREAM (también conocido como INCONTROLLER).

El Dr. Guri no es ajeno a la creación de técnicas novedosas para extraer datos confidenciales

de redes fuera de línea, y el investigador ha inventado cuatro enfoques diferentes desde inicios de 2020 que aprovechan varios canales secundarios para desviar información de forma subrepticia.

Estos incluyen BRIGHTNESS (brillo de pantalla LCD), POWER-SUPPLaY (fuente de alimentación), AIR-FI (Señales WiFi) y LANtenna (cables Ethernet). El último enfoque no es distinto, ya que aprovecha el cable Serial ATA para lograr los mismos objetivos.

Serial ATA es una interfaz de bus y un estándar Integrated Drive Electronics (IDE) que se utiliza para transferir datos a velocidades más altas a dispositivos de almacenamiento masivo. Uno de sus principales usos es conectar unidades de disco duro (HDD), unidades de estado sólido (SSD) y unidades ópticas (CD/DVD) a la placa base de la computadora.

A diferencia de violar una red tradicional por medio de spear-phishing o abrevaderos, comprometer una red aislada requiere estrategias más complejas, como un ataque a la cadena de suministro, el uso de medios extraíbles (por ejemplo, USBStealer y USBFerry) o infiltrados maliciosos para plantar malware.

Para un adversario cuyo objetivo es robar información confidencial, datos financieros y propiedad intelectual, la penetración inicial es solo el comienzo de la cadena de ataque seguida por el reconocimiento, la recopilación y la filtración de datos por medio de estaciones de trabajo que contienen interfaces SATA activas.

En la fase final de recepción de datos, los datos transmitidos se capturan por medio de un receptor oculto o confían en un miembro malicioso de una organización para llevar un receptor de radio cerca del sistema de espacio de aire.

> *«El receptor monitorea el espectro de 6 GHz en busca de una transmisión potencial, demodula los datos, los decodifica y los envía al atacante»,* dijo el Dr. Guri.

Como contramedidas, se recomienda tomar medidas para evitar que el actor de la amenaza obtenga un punto de apoyo inicial, usar un sistema de monitorea de radiofrecuencia (RF) externo para detectar anomalías en la banda de frecuencia de 6 GHz del sistema de espacio de aire, o alternativamente, contaminar la transmisión con operaciones aleatorias de lectura y escritura cuando se detecta una actividad sospechosa en un canal encubierto.