Cuatro diferentes frameworks maliciosos diseñados para atacar redes con brecha de aire fueron detectadas en la primera mitad de 2020, lo que elevó el número total de dichos conjuntos de herramientas a 17 y ofreció a los adversarios un camino hacia el ciberespionaje y la exfiltración de información clasificada.

> *«Todos los marcos están diseñados para realizar algún tipo de espionaje, y todos los marcos utilizan unidades USB como medio de transmisión físico para transferir datos dentro y fuera de las redes con espacio de aire específicas»*, dijeron los investigadores de ESET, Alexis Dorais-Joncas y Facundo Muñoz.

El espacio aéreo es una medida de seguridad de la red diseñada para evitar el acceso no autorizado a los sistemas, mediante un aislamiento físico de otros redes no seguras, incluyendo las redes de área local y la Internet pública. Esto también implica que la única forma de transferir datos es mediante la conexión de un dispositivo físico, como unidades de USB o discos duros externos.

Debido a que el mecanismo es una de las formas más comunes en que se protegen los sistemas SCADA y los Sistemas de Control Industrial (ICS), los grupos de APT que son patrocinados o forman parte de los esfuerzos de los estados nacionales, han puesto cada vez más su mirada en la infraestructura crítica con la esperanza de infiltrarse en una red de aire interrumpida con malware para vigilar objetivos de interés.

Construido principalmente para atacar sistemas operativos basados en Windows, ESET dijo que no menos del 75% de todos los marcos se encontraron aprovechando archivos maliciosos LNK o AutoRun en unidades USB para llevar a cabo el compromiso inicial del sistema con espacio de aire o moverse lateralmente dentro de la red con espacio de aire.

Algunos frameworks que se han atribuido a actores de amenazas conocidos son:

- Retro (DarkHotel, también conocido como APT-C-06 o Dubnium)
- Ramsay (DarkHotel)
- USBSteler (APT28 aka Sednit, Sofacy o Fancy Bear)
- USBFerry (Tropic Trooper, también conocido como APT23 o Pirate Panda)
- Fanny (Equation Group)
- USBCulprit (Goblin Panda, también conocido como Hellsing o Cycldek)
- PlugX (Mustang Panda)
- Agent.BTZ (Turla Group)

> *«Todos los frameworks han ideado sus propios métodos, pero todos tienen una cosa en común: sin excepción, todos usaban unidades USB armadas. La principal diferencia entre los marcos conectados y fuera de línea es cómo la unidad se arma en primer lugar»,* dijeron los investigadores.

Mientras que los marcos conectados funcionan mediante la implementación de un componente malicioso en el sistema conectado que monitorea la inserción de nuevas unidades USB y coloca de forma automática en ellas el código de ataque necesario para envenenar el sistema con espacio de aire, los marcos fuera de línea como Brutal Kangaroo, EZCheese y ProjectSauron, se basan en que los atacantes infectaron de forma deliberada sus propias unidades USB para crear backdoors en las máquinas objetivo.

De este modo, la transmisión encubierta de datos fuera de entornos con espacios de aire sin que los USB sean un hilo común sigue siendo un desafío. Aunque se han ideado varios métodos para desviar de forma sigilosa los datos altamente sensibles aprovechando los cables Ethernet, las señales WiFi, la fuente de alimentación de la computadora, e incluso los cambios en el brillo de la pantalla LCS como canales laterales novedosos, los ataques en la naturaleza que explotan esta técnica aún no se han observado.

Se recomienda a las organizaciones con sistemas de información críticos e información confidencial que eviten el acceso directo al correo electrónico en los sistemas conectados, deshabiliten los puertos USB y desinfecten las unidades USB, restrinjan la ejecución de

archivos en las unidades extraíbles y realicen análisis periódicos de los sistemas con espacio de aire para detectar cualquier señal de actividad sospechosa.

> *«Mantener un sistema completamente con espacio de aire cuenta con los beneficios de una protección adicional. Pero al igual que todos los demás mecanismos de seguridad, la brecha de aire no es una solución milagrosa y no evita que los actores malintencionados se aprovechen de los sistemas obsoletos o de los malos hábitos de los empleados»,* dijo Dorais-Joncas.