Los investigadores de seguridad cibernética están alertando sobre una ola continua de ataques vinculados a un grupo de amenazas rastreado como Raspberry Robin, que está detrás de un malware de Windows con capacidades similares a las de un gusano.

Al describirlo como una amenaza *«persistente y difundida»,* Cybereason dijo que observó una serie de víctimas en Europa.

Las infecciones involucran un gusano que se propaga por medio de dispositivos USB extraíbles que contienen un archivo .LNK malicioso y aprovecha los dispositivos de almacenamiento conectado a la red (NAS) de QNAP comprometidos para el comando y control. Fue documentado por primera vez por investigadores de Red Canary en mayo de 2022.

También llamado QNAP Worm by Sekoia, el malware aprovecha un binario de instalación legítimo de Windows llamado «msiexec.exe» para descargar y ejecutar una biblioteca compartida maliciosa (DLL) desde un dispositivo QNAP NAS comprometido.

> *«Para que sea más difícil de detectar, Raspberry Robin aprovecha las inyecciones de procesos en tres procesos legítimos del sistema Windows. Se comunica con el resto de la infraestructura de los nodos de salida TOR»,* dijo el investigador de Cybereason Loïc Castel.

La persistencia en la máquina comprometida se logra haciendo modificaciones en el Registro de Windows para cargar la carga útil maliciosa a través del binario de Windows «rundll32.exe» en la fase de inicio.

La campaña, que se cree que data de septiembre de 2021, sigue siendo un misterio hasta el momento, sin pistas sobre el origen del actor de amenazas o sus objetivos finales.

La divulgación se produce cuando QNAP dijo que está investigando activamente una nueva ola de infecciones de ransomware Checkmate dirigidas a sus dispositivos, lo que lo convierte en el último de una serie de ataques después de AgeLocker, eCh0raix y DeadBolt.

> *«La investigación preliminar indica que Checkmate ataca a través de servicios SMS expuestos a Internet y emplea un ataque de diccionario para romper cuentas con contraseñas débiles»,* dijo la compañía.

> *«Una vez que el atacante inicia sesión exitosamente en un dispositivo, cifra los datos en las carpetas compartidas y deja una nota de rescate con el nombre de archivo «!CHECKMATE_DECRYPTION_README» en cada carpeta».*

Como precaución, la empresa taiwanesa recomienda a los clientes que no expongan los servicios SMB a Internet, mejoren la seguridad de la contraseña, realicen copias de seguridad periódicas y actualicen el sistema operativo QNAP a la última versión.