Investigadores de seguridad cibernética descubrieron un nuevo malware de Windows con capacidades similares a las de un gusano, que se propaga por medio de dispositivos USB extraíbles.

Al atribuir el malware a un grupo llamado *«Raspberry Robin»*, los investigadores de Red Canary dijeron que el gusano *«aprovecha Windows Installer para llegar a los dominios asociados con QNAP y descargar una DLL maliciosa».*

Al parecer, los primeros signos de actividad se remontan a septiembre de 2021, con infecciones observadas en organizaciones vinculadas a los sectores tecnológico y manufacturero.

Las cadenas de ataque relacionadas con Raspberry Robin comienzan con la conexión de una unidad USB infectada a una máquina con sistema Windows. La carga útil del gusano se encuentra dentro del dispositivo, que aparece como un archivo de acceso directo .LNK a una carpeta legítima.

Después, el gusano se encarga de generar un nuevo proceso utilizando cmd.exe para leer y ejecutar un archivo malicioso almacenado en la unidad externa.

A esto le sigue el lanzamiento de explorer.exe y msiexec.exe, el último de los cuales se utiliza para la comunicación de red externa a un dominio no autorizado para fines de comando y control (C2) y para descargar e instalar un archivo de biblioteca DLL.

La DLL maliciosa se carga y ejecuta posteriormente mediante una cadena de utilidades legítimas de Windows, como fodhelper.exe, rundll32.exe y odbconf.exe, omitiendo efectivamente el Control de Cuentas de Usuario (UAC).

También es común en las detecciones de Raspberry Robin la presencia de contactos C2 saliente que involucran los procesos regsvr32.exe, rundll32.exe y dllhost.exe a las direcciones IP asociadas con los nodos Tor.

Los objetivos de los operadores siguen sin respuesta en esta etapa. Tampoco está claro cómo y dónde se infectan las unidades externas, aunque se sospecha que se lleva a cabo sin conexión.

> *«Tampoco sabemos por qué Raspberry Robin instala una DLL maliciosa. Una hipótesis es que puede ser un intento de establecer la persistencia en un sistema infectado»,* dijeron los investigadores.