Hundreds of Windows Networks Are Infected With Raspberry Robin Worm

By Matthew Humphries

July 4, 2022

It's unclear what the infected networks will be used for as no attack has been staged yet.

Microsoft released a private threat intelligence advisory informing organizations that a worm called Raspberry Robin is infecting hundreds of Windows networks.

As BleepingComputer reports(Opens in a new window), Raspberry Robin is being spread via infected USB devices. It requires a user to insert the USB device and click a malicious .LNK file. After that, the worm uses the Windows command prompt to launch an msiexec process and run a malicious file also present on the device.

A connection is then established with a command and control server using a short URL, and if successfuly, a number of malicious DLLs are downloaded and installed. The legitimate Windows utility odbcconf.exe is then used to execute the DLLs while the worm repeatedly attempts to connect to Tor network nodes. At least some of the command and control servers being used are thought to be infected QNAP NAS devices.

What's worrying is, whoever deployed Raspberry Robin so successfully has yet to take advantage of the infected Windows networks. The malware introduced by the worm is capable of bypassing Windows User Account Control (UAC) and has already proven it can use the utilities available to the OS. So while nobody currently knows the goal of Raspberry Robin, the control it imposes over a network means new malware could be downloaded and deployed very quickly.