Severity

High

Analysis Summary

Raspberry Robin is a new Windows virus found by researchers having worm-like capabilities that spreads via removable USB devices. Raspberry Robin makes use of Windows Installer to connect to QNAP-related domains and download a malicious DLL. TOR exit nodes are used as a backup C2 infrastructure by this malware. Raspberry Robin was first discovered in September 2021. This malware is observed targeting companies in the technology and manufacturing industries. The Raspberry Robin worm appears as a shortcut .lnk file masquerading as a legitimate folder on the infected USB device. The UserAssist registry item is updated shortly after the Raspberry Robin infected disc is attached to the system, and when decoded, it records the execution of a ROT13-ciphered value referencing a.lnk file. For example q:\erpbirel.yax deciphers to d:\recovery.lnk. Raspberry Robin reads and executes a file from the infected external drive using cmd.exe and it utilizes msiexec.exe for external network communication to a rogue domain used as C2 to download and install a DLL library file. After that msiexec.exe runs fodhelper.exe, a Windows utility, which runs rundll32.exe to run a malicious operation. Fodhelper.exe processes run with elevated administrator rights without necessitating a User Account Control prompt, according to experts.

Impact

- Exposure of Sensitive Data
- Unauthorized Access

Indicators of Compromise

MD5

- 6f5ea8383bc3bd07668a7d24fe9b0828
- e8f0d33109448f877a0e532b1a27131a

SHA-256

- 1a5fcb209b5af4c620453a70653263109716f277150f0d389810df85ec0beac1
- c0a13af59e578b77e82fe0bc87301f93fc2ccf0adce450087121cb32f218092c

SHA-1

- 90e00d255fc9162080c02510e7e10ffa6b6ed995
- bfcfa72ba5095fba108314c1c4deb5faed82ef4d

Remediation

- Block all threat indicators at your respective controls.
- Search for IOCs in your environment.