# Detecting a new strain of malicious code that abuses Windows Installer to deploy infection activities

Security researchers at Red Canary have discovered a new Windows malware capable of spreading by means of an external USB drive. This malware is associated with an agent group called Raspberry Robin, which was first observed in September 2021.

Currently, this malicious code is found in the network of a series of global organizations and businesses, mainly operating in the fields of technology and manufacturing.

Preliminary investigation results from Red Canary show that Raspberry Robin spreads to target Windows systems when an infected USB drive contains a malicious .LNK file. Once attached, it creates a new process using cmd.exe to launch a malicious file hosted in-place.

Raspberry Robin abuses Microsoft Standard Installer (msiexec.exe) to gain access to its control and control servers (C2 server). The malicious code is likely hosted on compromised QNAP devices and uses TOR exit nodes as additional C2 infrastructure.

"While msiexec.exe downloads and executes legitimate installer packages, malicious actors also leverage it to distribute malicious code. Raspberry Robin uses msiexec.exe to attempt to communicate externally with an external network malicious domain for control and control purposes," Red Canary said.

The team suspects that Raspberry Robin installs malicious DLL files on compromised systems to prevent them from being deleted between reboots. It launches this DLL file with the help of 2 other legitimate Windows utilities: fodhelper (a trusted binary for managing features in Windows Settings) and odbcconf (a tool for configuring ODBC drivers). ). fodhelper will allow malicious code to bypass User Account Control (UAC), while odbcconf will help execute and configure the DLL.


Although the Red Canary team has conducted close testing on the infected systems, there are still some questions that need to be answered.

First and foremost, researchers have yet to determine how or where Raspberry Robin was able to infect external drives to keep it functioning. While this could theoretically happen in an offline environment, the odds are not high.

'We also don't know why Raspberry Robin installed a malicious DLL,' the Red Canary researchers said. "One theory is that this could be an attempt by malicious code to establish persistence on an infected system. However, additional information will be needed to build confidence in that hypothesis."

Since there is no information about the malicious activities at the end of Raspberry Robin, there is one more question that needs to be answered: What is the real goal of the malicious code operators'. These will be conundrums that researchers must clarify step by step!