Abstract

Cryptojacking (also called malicious cryptocurrency mining or cryptomining) is a new threat model using CPU resources covertly "mining" a cryptocurrency in the browser. The impact is a surge in CPU Usage and slows the system performance. In this research, in-browser cryptojacking mitigation has been built as an extension in Google Chrome using Taint analysis method. The method used in this research is attack modeling with abuse case using the Man-In-The-Middle (MITM) attack as a testing for mitigation. The proposed model is designed so that users will be notified if a cryptojacking attack occurs. Hence, the user is able to check the script characteristics that run on the website background. The results of this research show that the taint analysis is a promising method to mitigate cryptojacking attacks. From 100 random sample websites, the taint analysis method can detect 19 websites that are inflected by cryptojacking.