Abstract

This research builds a model of in-browser-mitigation using extensions on Google Chrome against cryptojacking using the Taint Analysis method. Cryptojacking (also called malicious 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 slow the system performance. 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 design of the proposed model can notify user if a cryptojacking attack occurs. That way the user can find out the script characteristics that run on the website background. The results of this study can mitigate cryptojacking attacks, from 100 random sample websites the proposed model can detect 19 websites indicated cryptojacking. Keywords: cryptomining, cryptocurrency, taint analysis, MITM, mitigation, cryptojacking, abuse case.

Kata kunci :cryptomining, cryptocurrency, taint analysis, MITM, mitigasi, cryptojacking, abuse case.