
Abstrak

Penelitian ini membuat perancangan model in-browser-mitigation menggunakan ekstensi pada Google Chrome terhadap cryptojacking dengan metode Taint Analysis. Cryptojacking (juga disebut malicious cryptomining) adalah threat model baru menggunakan resource CPU secara sembunyi untuk "mining" suatu cryptocurrency pada browser. Dampaknya berupa kenaikan CPU Usage dan performa sistem yang lambat. Metode yang digunakan pada penelitian ini adalah pemodelan serangan dengan abuse case menggunakan teknik penyerangan Man-In-The-Middle (MITM) sebagai acuan untuk mitigasi. Perancangan model yang diusulkan dapat memberikan notifikasi kepada pengguna browser jika serangan cryptojacking terjadi. Dengan begitu pengguna dapat mengetahui karakteristik skrip yang berjalan pada background website. Hasil dari penelitian ini dapat memitigasi serangan cryptojacking, dari 100 sampel random website, model yang diajukan dapat mendeteksi 19 website yang terindikasi menginjeksi cryptojacking.

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