HEURISTIC METHOD OF CODE ANALYSIS

Abstract

A method of detecting malware at a computing device. The method includes examining a software program comprising a sequence of program instructions, determining whether each instruction in the sequence meets any of a group of suspicion criteria, assigning a instruction-level score to each instruction that meets any of the suspicion criteria, summing the instruction- level scores for each instruction to yield a program-level score, determining whether the program-level score exceeds a threshold, and, if the program-level score exceeds a threshold, developing a report indicating a malware detection result.

Figure 3