N/A and signature analysis for malwares detection and removal

ABSTRACT

Objectives: This study aimed to design an application that effectively scans, detects, and removes malware based on their signatures and behaviours. Methods/Statistical analysis: The rapid growth in the number and types of malware poses high security risks despite the numerous antivirus softwares with Signature-Based Detection (SBD) method. The SBD method depends on the signatures or malware names that are available in the algorithm database. Findings: Malware is a type of malicious software that poses security threats to the targeted system, resulting in information loss, resource abuse, or system damage. The antivirus software is one of the most commonly used security tools to detect and remove malware. However, the malware defences should focus on the malware signatures since there is no universal way of recognising all malware. Therefore, this study suggested N/A detection technique as the dynamic method (behaviour-based detection method) that depends on the Windows Registry (system database). Both static and dynamic detection methods were assessed in this study. Based on the experimental outcomes, SBD method detected and removed most of malware (only known viruses). Application/Improvements: Meanwhile, the N/A detection method detected and removed all injected malware (known and unknown Trojan horse) within a relatively low running time.

Keyword: Dynamic method; Malicious software; Malware detection; Signature analysis; Static method