

ABSTRACT

ANTIVIRUS CHARACTERISTICS ANALYSIS BASED ON COMPUTATION RESOURCE METRIC AND DETECTION INDIKATORS

By

Ramiz Qudamah

1202190065

Malware, short for "malicious software", is a process that can be prevented, searched for, detected and removed using antivirus software. This study aims to identify the characteristics of antivirus based on malware analysis and antivirus analysis. Malware analysis includes the number of blacklist strings, file ratio, sections, libraries, functions. Antivirus analysis includes computing resources such as CPU, memory, disk usage, as well as scan times and detection rates. This research does not discuss the internal system of the antivirus and does not discuss the source code. There are 6 samples of malware which are trojan, ransomware, and downloader types. The experimental platform is in the form of virtualization scanning malware on antivirus on a laboratory scale. The experiment was carried out by running the malware on a Windows 8.1 desktop environment in a virtual machine. Then do the scanning by antivirus by monitoring computing resources using the Task Manager and Personal User Activity applications. The experimental results are measured on computing resources such as CPU usage, memory, disk, and scan time. In the antivirus features tested, the Avast antivirus uses relatively lower computing resources, which is around 15.50% on the CPU, and 22.5 Megabytes on the memory. McAfee has the lowest scan time with a time of 9.17 seconds. McAfee Antivirus is relatively the highest in detecting malware samples with a detection rate of 100%. The results showed that the higher the value of the detection metric on malware, the higher the value of the metric tested on the antivirus. The continuation of this research can be in the form of adding malware samples, variations of malware types and adding anti-virus metrics.

Keywords: *Characteristics, Profiling, Real-time Protection, Testing, Detection Level*