ABSTRACT

MALWARE ANALYSIS BASED ON CALL MEMORY API WITH SIGNATURE-BASED DETECTION METHOD

By

JULIAN DWI NUGRAHA

1202154120

Malware is a software or computer program that is used to commit a crime. Malware is basically designed to infect user computer systems without the owner's consent. Trojans, Worms, Viruses, Spyware, and Keyloggers are categories of malware that can harm infected users. Based on this, the analysis malware is used using the API call memory with the signature-based detection method. Signature-based detection is a detection technique based on pattern matching, strings, masks, or fingerprinting techniques. Signature is a bit equation technique that is injected into an application program by an attacker, which uniquely identifies certain types of malware. This is used with the aim of identifying the malware containing a program that can retrieve user data without the user's knowledge. Therefore, in this study, malware analysis was carried out using as many as 150 malware samples and those importing API memory indicated containing 30 malware. This study focuses on analyzing the API Memory that has been obtained. Of all malware will run the same API memory when running the first time. The results of this study are to see the call memory API and the results of the signatures that have been done using the signature-based detection method and see the relationship between the call memory API and the results of the signatures on each malware.

Keyword : *malware, malware analysis, static analysis, dynamic analysis, signature-based*