ABSTRACT

IMPACT ANALYSIS OF MALWARE BASED ON CALL NETWORK API WITH HEURISTIC DETECTION METHOD

By

ONE TIKA SURYATI

1202154320

Malware is a program that has a negative influence on computer systems that do not have user permissions. The growing world of the internet, the more the number and types of malware are growing. The purpose of making malware by hackers is to make money in an illegal way. With the existence of these dangers make the computer users feel threatened. Therefore we need a malware analysis. Malware analysis aims to determine the specifics of malware so that it can improve security on a computer system. Many methods can be used in analyzing malware, one of which is the heuristic detection method. Heuristic detection is an analytical method that allows finding new types of malware by looking for commands or instructions that should not be found in an application. With the advancement of technology, more and more people will access the internet, so that a lot of malware is made to attack through the internet. Based on these conditions, the malware analysis is carried out using the API call network with the heuristic detection method. This aims to identify how the tendency of malware to attack from the network side. The results of the analysis of this study are malware with the API network tends to be spyware, which is lurking activities and retrieving user data without the user's permission. In addition, there is also malware that is adware, which displays advertisements through pop-up windows on computer devices that can interfere with user activity. So that with these results, we can identify the actions that must be taken by the user to protect his computer device, such as by installing antivirus or antimalware, not downloading unauthorized applications and not accessing unsafe websites.

Keywords : *malware, malware analysis, heuristic detection,* API *call network.*