ABSTRACT

Every day there are various types of new malware on the Internet. Where the technology used malware is growing. Malware already uses various techniques and ways to trick the antivirus when it infects the victim. The development of malware should be offset by doing research on malware detection. Therefore, in this study conducted malware analysis activities using as many as 170 malware to do the category based on its malicious activity. Malicious activity can be seen from the type of API call used. In this study using 3 (three) types of API call API file, API process and API registry. Techniques used to obtain API call information are Static Analysis and Dynamic Analysis. So the results obtained there are 5 categorizations with a minimum of 0 combinations and a maximum of 5 combinations of malicious activity. Where in this analysis using clustering method that is divided into 3 clusters that have more than 1 (one) combination of malicious activity. The impact analysis provided depends on the number of combinations, the more API API combinations the greater the impactny on the infected computer. In this study the impact given is high because there are malware that has 2 (two) combinations up to 5 (five) combination of malicious activity.

Keyword : *malware, malware analysis, static analysis, dynamic analysis, clustering*