ABSTRACT

Malware is a program or software that aims to enter into the computer system without the knowledge of its users and can interfere with or even damage the computer system. Over time, the types and threats of malware increasingly sophisticated and widespread. The spread of malware can be through various ways and one of the ways is the malware creator to insert the malware program into various types of files and then pack it in order to fool antivirus so malware program is not detected, then when the user run or open the malware-inserted file then automatically malware program will be active and infect the user's computer.

Therefore, this study was conducted to detect and analyze the sample files that allegedly inserted malware. This research is run in a virtual machine with remnux operating system which in the operating system have available sample of malware and tools to be able to perform surgery on sample file which will be detected and analyzed. In this study the authors use the anomaly method with static techniques to find the anomaly of the sample files that will be researched. This static technique does not execute malware samples, but only dissect it. Sample File to be researched in the form of .exe file and pdf file. In each type of file extension there will be two samples of different files that are clean of malware and malware inserted, then compared what anomalies are in both files.

In this research, the stages of the anomaly method that will be done is the phase of training, learning, and analysis. The output of this research is a fileprint table of anomalies in the sample files that have been researched, and is expected to help the understanding of malware and in reducing and preventing cybercrime in cyberspace.

Keywords: *malware, malware analysis, anomaly method, static analysis,* remnux.