ABSTRACT

Reports of malware attacks continue to rise, compelling researchers to consistently advance and innovate in mitigating, preventing, and eradicating malware attacks. On the other hand, malware developers are also determined not to be left behind, they continue to evolve and innovate by utilizing anti-forensic tools in the form of program packers for data hiding. Although program packers fall under the category of anti-forensic tools, they can also be beneficial in maintaining the integrity and validity of code by employing packing functions, thus complicating the reverse engineering process. Therefore, this final project (ta) conducts research on program packers as anti-forensic tools in malware attacks. The objectives of this research are to determine the impact of using program packers on the capabilities of digital forensic detection and analysis and to identify steps to address the impacts produced by program packers. The methods employed in this research include static analysis and dynamic analysis. Static analysis utilizes reverse engineering methods as a means of obtaining information about the components of malware, while dynamic analysis involves executing malware in a secure environment to directly observe its behavior. This research is expected to provide new insights into the domain of malware analysis, emphasizing the importance of understanding program packers as anti-forensic tools in digital forensic investigations of malware samples.