A STATIC AND DYNAMIC HEURISTIC ANALYSIS TO CALCULATE MALWARE THREAT SCORE

By

Reischaga

11602015

BACHELOR'S DEGREE

in

INFORMATION TECHNOLOGY

ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
Alam Sutera
Tangerang 15339
Indonesia

June 2020

Revision after the Thesis Defense on 14th July 2020

STATEMENT BY THE AUTHOR

I hereby declare that this submission is my own work and to the best of my knowledge, it contains no material previously published or written by another person, nor material which to a substantial extent has been accepted for the award of any other degree or diploma at any educational institution, except where due acknowledgement is made in this thesis.

Reischaga

Student Date

Approved by:

Dr. Charles Lim, M.Sc.

Thesis Advisor Date

Mr. Yohanes Syailendra Kotualubun, M.Kom.

Thesis Co-Advisor Date

Maulahikmah Galinium, S.Kom, M.Sc, PhD,

Dean Date

ABSTRACT

A STATIC AND DYNAMIC HEURISTIC ANALYSIS TO CALCULATE MALWARE THREAT SCORE

By
Reischaga
Dr. Charles Lim, M.Sc., Advisor
Mr. Yohanes Syailendra Kotualubun, M.Kom., Co-Advisor

SWISS GERMAN UNIVERSITY

Malware can be defined as any software that performs malicious actions without the consent of the user. The volume of malware is increasing every year and the threat it poses is only becoming ever more prevalent. Currently, malware is involved in a large portion of security incidents, of which are currently handled without a threat level metric system. In this study, we demonstrate how static analysis and dynamic analysis could be utilized, both separately and combined, effectively in order to quantitatively assess malware threats by calculating their threat scores.

Keywords: Malware, Dynamic Analysis, Static Analysis, ATT&CK Framework, Threat Scoring

DEDICATION

I would like to dedicate this research project to my family and my beloved country Indonesia. Additionally, I wish to dedicate this work as a projection of the knowledge and mentor-ship given to me by my teachers and seniors, whom have tirelessly and selflessly taught me and answered my questions during the course of this research.

ACKNOWLEDGEMENT

First and foremost is to thank my mentors, family, friends, and God in giving relentless support until the completion of this thesis. I would like to express my gratitude to my advisor, as well as co-advisor for their support, patience and time. Dr. Charles Lim, M.Sc. was very helpful in guiding in analytical studies and gave very helpful insights and guidance in malware, as well as up to date situations and trends in the research world. Mr. Yohanes Syailendra Kotualubun, M.Kom. as my co-advisor had been very helpful in giving guidance and knowledge regarding static and dynamic analysis experimentations and scientific writing. Mr. Mario Marcello, S.Kom., B.Eng. and Alexander Suhandi, ST, M.Kom. had been helpful in providing insights into dynamic analysis. Last but not least, I would like to thank Mr. Ali Suwanda, S.Kom. as my research partner for his support throughout this thesis.

TABLE OF CONTENTS

List of Figures

List of Tables