MALWARE THREAT SCORE FRAMEWORK USING STATIC AND DYNAMIC FEATURES

By

Ali Suwanda

21851013

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

June 2020

MALWARE THREAT SCORE FRAMEWORK USING STATIC AND DYNAMIC FEATURES

By

Ali Suwanda

21851013

MASTER'S DEGREE

in

MASTER OF INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

SWISS GERMAN UNIVERSITY
The Prominence Tower
Jalan Jalur Sutera Barat No. 15, Alam Sutera
Tangerang, Banten 15143 - Indonesia

June 2020
Revision after the Thesis Defense on July 17 th 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 the thesis.

Ali Suwanda

Student Date

Approved by:

Dr. Charles Lim, BSc., MSc.

Thesis Advisor Date

Dr. Ir. Lukas, MAI.

Thesis Co-Advisor Date

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

Dean of Faculty of Engineering and Information Technology Date

ABSTRACT

MALWARE THREAT SCORE FRAMEWORK USING
STATIC AND DYNAMIC FEATURES

By

Ali Suwanda
Dr. Charles Lim, BSc., MSc. , Advisor
Dr. Ir. Lukas, MAI. , Co-Advisor

SWISS GERMAN UNIVERSITY

In recent study malware threat becomes more targeted over three years. With those indications, malware threat became a massive risk to the organization therefore, it is important for the organization to improve their situational awareness in cyber security context. It is important for the management to take a decision and create awareness to the organizations hence, threat score can provide high-level information of malware threat that can support strategic and decision making process in the organization. This study focus on to analyze data to create a threat score framework and measure their threat using static and dynamic analysis.

Keywords: Static Analysis, Dynamic Analysis, Threat Score.

DEDICATION

I would like to dedicate this research project to my family and my beloved country Indonesia.

ACKNOWLEDGEMENT

I would like to express my deepest gratitude to Dr. Charles Lim, BSc., MSc. and Dr. Ir. Lukas, MAI. as my thesis advisor and co-advisor for their relentless support and guidance during my research project. I wish to thank for Mr. Reischaga Mohajit as my discussion partner and support throughout this research. It is because of their contributions this thesis report and the whole research project can arrive at this point.

I would like to thank my family, especially to my brother Mr. Yohanes Christianto for their moral supports throughout my pursue of master degree in SGU. Finally, I would like to thank all of my direct supervisor, my team at work and my friends especially Batch 23 MIT SGU for their companionship, and to the countless number of people who have helped me throughout this research project, either directly or indirectly.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES