HIDDEN-CODE EXTRACTION FROM PACKED MALWARE USING MEMORY BASED DYNAMIC ANALYSIS

By

Yohanes Syailendra Kotualubun

22013211

In partial fulfillment of the requirements for the

MASTER'S DEGREE

in

INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

Swiss German University
EduTown BSDCity
Tangerang 15339
INDONESIA

March 2017

HIDDEN-CODE EXTRACTION FROM PACKED MALWARE USING MEMORY BASED DYNAMIC ANALYSIS

By

Yohanes Syailendra Kotualubun

22013211

In partial fulfillment of the requirements for the

MASTER'S DEGREE

in

INFORMATION TECHNOLOGY

FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY

Swiss German University
EduTown BSDCity
Tangerang 15339
INDONESIA

March 2017
Revision after Thesis Defense on February 16, 2017

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 acknowledgment is made in this thesis.

Yohanes Syailendra Kotualubun

Student Date

Approved by:

Adhiguna Mahendra, Ph.D

Thesis Advisor Date

Charles Lim, M.Sc

Thesis Co-Advisor Date

Dr. Ir. Gembong Baskoro, M.Sc

Dean Date

Abstract

Hidden-Code Extraction From Packed Malware Using Memory Analysis

By

Yohanes Syailendra Kotualubun

Adhiguna Mahendra, Ph.D, Advisor

Charles Lim, MSc., Co-Advisor

Swiss German University

Software packer has been used effectively to hide the original code inside a binary executable of any malware, making it more difficult for existing signature-based anti virus software to detect malicious code inside the executable. In this Thesis, we propose Mal-Xtract, a method to detect the end of unpacking routine and extract original code from packed binary executable using Memory Analysis running in an software emulated environment. The extracted code will be validated using similarity and entropy calculation that compare the extracted body with original body. Our experiment results show that at least 97% of the original code from the various packed executable with different software packers could be extracted.

Keywords: Packed Malware, Memory Forensic, Dynamic Analysis, Evasion technique, Emulation.

Dedication

I would like to dedicate this research project to my beloved country, Indonesia. I believe this thesis research can contribute to the advancement of science and technology in Indonesia, especially in Malware Research, no matter how subtle.

Acknowledgement

I would like to express my deepest gratitude to Mr Adhiguna Mahendra, Ph.D and Mr. Charles Lim for the time, support, advice, and guidance given throughout this research project and the completion of this thesis report. It is because of their priceless contributions that this thesis report and the whole research project can arrive at this point.

I would like to thank all of my friends for their companionship, and to the countless number of people who have helped me throughout this research project, either directly or indirectly.

Last, but the most important, I would like to thank my whole family for the countless moral supports throughout my life. It is because of their guidances that I become the person as who I am today. It is because of their affections that I become as happy as I am today.

Contents