

**EXTRACTION OF MALICIOUS CODE FROM PACKED MALWARE USING
EMULATED ENVIRONMENT**

By
Suhandi
21551009

MASTER'S DEGREE
in
MASTER OF INFORMATION TECHNOLOGY
FACULTY OF ENGINEERING AND INFORMATION TECHNOLOGY



Revision after the Thesis Defence on January 15th 2018

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

Januari 2018

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.

Suhandi

Student

Date

Approved by:

Dr. Ir. Lukas, MAI, CISA, IPM

Thesis Advisor

Date

SWISS GERMAN UNIVERSITY

Charles Lim, BSc., MSc., CHFI, EDRP,
ECSA, ECSP, ECIH, CEH, CEI

Thesis Co-Advisor

Date

Dr. Irvan Setiadi Kartawiria, S.T.,M.Sc.

Dean of Faculty of Engineering and Informa-
tion Technology

Date

ABSTRACT

EXTRACTION OF MALICIOUS CODE FROM PACKED MALWARE USING EMULATED ENVIRONMENT

By

Suhandi

Dr. Ir. Lukas, MAI, CISA, IPM , Advisor

Charles Lim, BSc., MSc., CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI , Co-Advisor

SWISS GERMAN UNIVERSITY

Malware Authors are nowadays creating a new technique for evading malware analyst. Encryption and compression can evade a malware static analysis. Binary Obfuscation is one of the techniques which applied encryption and compression on malware. In this thesis, a method is proposed to perform a dynamic analysis from packed malware using memory scanning analysis and instruction tracing to extract a hidden code of malware. By using this method, unpacking process can be determined exactly and hidden code can be extracted. Using similarity and entropy as validation technique help analyst to determine whether hidden malicious code can be extracted successfully.

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



SWISS GERMAN UNIVERSITY

DEDICATION

I would like to dedicate this research project to my God, my family, my beloved country Indonesia and my second home where I grow in knowledge, PT Astra Graphia Information Technology.



ACKNOWLEDGEMENT

I would like to express my deepest gratitude to Dr. Ir. Lukas, MAI, CISA, IPM and Mr. Charles Lim, BSc., MSc., CHFI, EDRP, ECSA, ECSP, ECIH, CEH, CEI as my Thesis advisor, for Mr. Yohanes Kloatubun as my mentor and discussion partner 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 my wife and daughter for the countless moral supports throughout my pursue of knowledge in SGU. I can't thank you enough for the time that already taken from you for me to make this thesis done.

I would like to thank all of my direct supervisor, my team at work and my friends especially Batch 17 MIT SGU for their companionship, and to the countless number of people who have helped me throughout this research project, either directly or indirectly.



SWISS GERMAN UNIVERSITY

Table of Contents

	Page
STATEMENT BY THE AUTHOR	1
ABSTRACT	2
DEDICATION	4
ACKNOWLEDGEMENT	5
TABLE OF CONTENTS	8
LIST OF FIGURES	9
LIST OF TABLES	10
1. INTRODUCTION	11
1.1 Background	11
1.2 Problem Statement	13
1.3 Research Objective	13
1.4 Research Question	14
1.5 Scope and Limitation	14
1.6 Significance of Study	15
2. LITERATURE REVIEW	16
2.1 Malware	16
2.1.1 Malware Definition and History	16
2.1.2 Malware Trends	18
2.2 Malware Detection	19
2.3 Malware Obfuscation Techniques	21

2.3.1	Portable Executables	21
2.3.2	Stealth Malware Techniques	22
2.3.3	Encryption	22
2.3.4	Oligomorphism	23
2.3.5	Polymorphism	23
2.3.6	Metamorphism	26
2.3.7	Code Packing	26
2.4	Malware Analysis	28
2.4.1	Static Analysis	29
2.4.2	Dynamic Analysis	31
2.4.3	Dynamic Binary Instrumentation	34
2.4.4	Dynamic Binary Unpacking	36
2.5	Entropy Analysis	36
2.6	String Similarity Analysis	37
2.6.1	Levensthein Distance	38
2.6.2	Longest Common Subsequence	38
2.6.3	Normalized Compression Distance (NCD)	38
2.7	Related Works	39
2.8	Contribution	42
3.	RESEARCH METHODS	44
3.1	Research Framework	44
3.2	Algorithm of Framework	45
3.2.1	Collection of Samples	45
3.2.2	Create Recording	46
3.2.3	Trace Execution and Collection of Logs	46
3.2.4	Analyze Trace Execution and Memory Write Logs	46
3.2.5	Extracting Hidden Executables	47
3.2.6	Hidden Executables Extraction Validation	49
4.	RESULTS AND DISCUSSIONS	51
4.1	Experiment Setup	51
4.1.1	Hardware Setup	51

4.1.2 Software Setup 51

4.2 Dataset 52

4.3 Results and Analysis 53

4.3.1 Benign Experiment Results 53

4.3.2 Malware Experiment Results 56

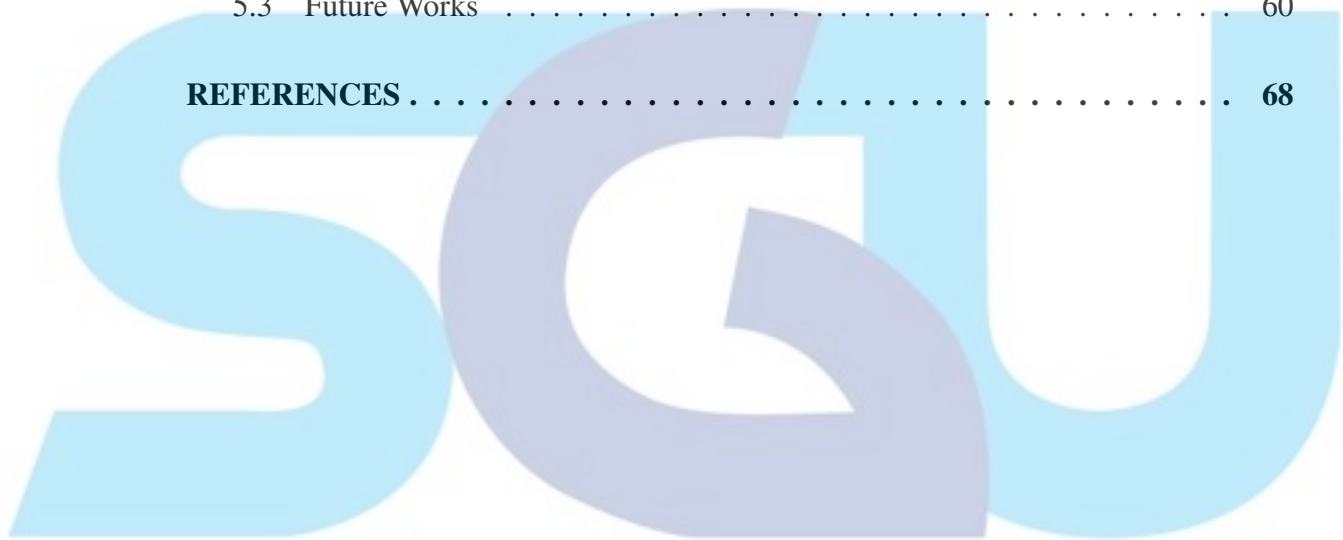
5. CONCLUSIONS AND RECCOMENDATIONS 60

5.1 Conclusions 60

5.2 Reccomendations 60

5.3 Future Works 60

REFERENCES 68



SWISS GERMAN UNIVERSITY