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

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 Information 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

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.

Table of Contents