UNIVERSITI TEKNOLOGI MARA

MANUAL MALWARE ANALYSIS USING STATIC AND DYNAMIC METHODS

ARIFIN BIN SALLEH

Dissertation submitted in partial fulfilment of the requirement

for the degree of

Master of Science (Computer Networking)

Faculty of Computer & Mathemathical Science

JANUARY 2013

ACKNOWLEDGEMENT

In the name of Allah, the Most Gracious and Merciful. With His permission, this study has been completed. I would like to convey my deepest appreciation to all individuals who have contributed and help me in finishing this dissertation. I am very thanful to my supervisor, Puan Norkhusaini Awang for he precious time, guindance and advices throughout the research period.Besides, I wish to express thanks to all lecturers for their guidance, advice and opinions in improving quality of this dissertation.

Finally I would like to deliver sincere gratitude to my beloved wife, Jasmiah Jaffar, my daugthers Amirah Syamimi, Amirah Zahidah, my son Muhammad Adib, beloved parent, the whole family and friends for their support motivation during period of study at UiTM shah Alam Selangor.

ABSTRACT

Today, malware threats are an important topic of security threat research. Combat between malware writer and malware researcher never end. Malware writers use a variety of avoidance techniques such as Code Obfuscation, Packing, Anti-Debugging and Anti-Virtualization Technologies to foil researcher's analysis. On behalf of researchers they try to find out many techniques to defend IT information services from access or stolen by unauthorized parties. Most of the researches today perform malware analysis in Virtualization Technology in the isolation environment because of security issues. This study focuses on analysis malware using combined static and dynamic in Operating System environment. Thus we focus on malware analysis that uses Anti-Virtualization avoidance technique. Although our platform environment exposed to the threat by malware sample, we protect this environment by using Toolwiz TimeFreeze and window backup image to protect or secure our environment. We took 20 samples of malware from different types of analysis in this environment. We prove that our environment capable to do malware analysis and compare our environment with the virtual machine environment to prove that our analysis more accurate.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

1.0 Introduction

Now day malware threats were assessed by IT security organizations has been growing more than ten thousand every day. By using many avoidance techniques such as self-defending code, packing, anti-debugging and anti-Virtualization techniques, these flood complex threats has a leading cause of many problems on computer network especially cause of bottlenecks in the network and increased threat of criminal for corporate and individual data. The most challenging for antivirus organization and researcher today is about the threat that occurs in computer application because of the unknown vulnerability or known as a zero-day attack. This attack will take advantage of an application that have issue of security vulnerability.

Malware analysis today still relevant to analyze these threats for the purpose of understanding the problem such as what the entry method and what it did into the host? How to solve the problem, and ensure future threats does not compromise effective response. Symantec Internet Security Threat Report 2011 reveals that the total number unique variants of malware in the world in 2011 around 403 million compared to 286 million variants in 2010. Many machines already infected while the anti-malware firm discovered the malware. Most of anti-malware firm depend on signature base for detecting the variant of malware today and a little bit of them uses heuristic based detection. These reasons also contribute to researcher fine out the best