

TERMINATING RANSOMWARE ATTACK ON USER FILES IN WINDOWS

ENDPOINT

By

Abrão Ximenes

21551001

MASTER'S DEGREE

in

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

February 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.

Abrão Ximenes

Student

Date

Approved by:

Dr. Eka Budiarto, S.T., M.S

Thesis Advisor

Date

SWISS GERMAN UNIVERSITY

Charles Lim, BSc., MSc.

Thesis Co-Advisor

Date

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

Dean of Faculty of Engineering and Information Technology

Date

ABSTRACT

TERMINATING RANSOMWARE ATTACK ON USER FILES IN WINDOWS ENDPOINT

By

Abrão Ximenes

Dr. Eka Budiarto, S.T., M.S , Advisor
Charles Lim, BSc., MSc. , Co-Advisor

SWISS GERMAN UNIVERSITY

Ransomware is one of the most phenomenal threats that facing by individuals, industries, organizations and Government nowadays. The type of this malware hostage user files, computers, mobile phone and other devices that connect to network and Internet to prevent users to access data and devices. This malware leverages the weaknesses of human, process and technology to carry out its attack.

This research proposed a method to terminate ransomware attack on user files in its early stage of encryption. We monitor file operations activities in file system using minifilter driver. Due to the behaviors of file operations that performed by ransomware are very different.

There are 10 family of ransomware and more than 313 ransomware samples were used during this research project. The experiment and evaluation indicated that the method proposed can success terminates the ransomware.

Keywords: Ransomware, user files monitoring, terminates ransomware activity, minifilter, minispy



SWISS GERMAN UNIVERSITY

DEDICATION

I would like to dedicate this research project to my beloved country, Timor Leste.



ACKNOWLEDGEMENT

First of all, I thank to my Almighty GOD, Jesus Christ, with all His grace and His favour which pour out upon me with healthy, ability, capacity and joyfully. I would like to express my deepest gratitude to Dr. Eka Budiarto, S.T., M.S and Mr. Charles Lim, BSc., MSc. as my Thesis advisor, for Mr. Yohanes Syailendra Kotualubun 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. I am also grateful to Mr. Ofer who is always willing to discuss about malware. Through their priceless contributions, the whole research project can arrive at this point.

I would like to thank to Mrs. Ayu Diana Lestari, Dr. Ir. Moh. A. Amin Soetomo, M.Sc, Dr. Eka Budiarto, S.T., M.Sc, Vice Rector Non-Academic Affairs Mr. Edward Boris P. Manurung, M.Eng, Pak Imam, SGU International Office Mrs. Mina Arsita who are always available to help me to arrange my immigration documents during doing research project and study at Swiss German University. If without their helps I could not stay in Indonesia to continue my study.

I would like to thank to all my friends for their companionship and to the countless number of people who have helped me throughout this research project, either directly or indirectly. I would like to thank to my whole beloved family, Brad & Dawn Grabs, Tom & Susie Ulrickson, Luis Soares and their family for the countless supports throughout my life. Through all of their guidance and support that I could become the person as who I am today.

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	12
1.3 Research Objective	13
1.4 Research Question	13
1.5 Scopes of Research	14
1.6 Significance of Study	14
1.7 Thesis Structure	14
2. LITERATURE REVIEW	15
2.1 Malware	15
2.2 Types of Malware	15
2.3 Ransomware	17
2.4 Ransomware Evolution	17

2.5	Type of Ransomware	21
2.5.1	Locker Ransomware	21
2.5.2	Crypto Ransomware	21
2.5.3	Crypto-Locker/Hybrid Ransomware	22
2.6	Anatomy of Ransomware Attack	22
2.6.1	Deployment	22
2.6.2	Installation	23
2.6.3	Command-and-Control Server	23
2.6.4	Destruction	24
2.6.5	Extortion	24
2.7	Common Encryption Algorithms Deployed by Ransomware	24
2.7.1	Symmetric Algorithms	25
2.7.2	Asymmetric Algorithms	25
2.7.3	Hybrid Algorithms	26
2.8	Resilience	26
2.9	Malware Analysis	27
2.9.1	Static Analysis	27
2.9.2	Dynamic Analysis	28
2.10	File System Filter Driver	28
2.11	File System Minifilter Driver	28
2.12	Related Works	30
3.	RESEARCH METHODS	36
3.1	Overview	36
3.2	Research Methodology	36
3.3	Research Framework -Kernel Level	37
3.3.1	Intercepts file operation in Files system	37
3.4	Research Framework API level	40
3.5	Dataset Collection	40
3.5.1	Ransomware Dataset	41
3.5.2	Benign Application	41
4.	RESULTS AND DISCUSSIONS	42

4.1	Environment Setup	42
4.1.1	Tools	43
4.2	Dataset	43
4.3	Minispy Filter Driver	44
4.4	Analysis	45
4.4.1	Ransomware Attack User Files	45
4.4.2	Locky Ransomware	45
4.4.3	Tesla Ransomware	47
4.4.4	Cerber Ransomware	47
4.4.5	Ransomware Comparison	48
4.4.6	Benign Application API Calls	49
4.5	Terminating Ransomware Attack	50
4.6	Evaluation	50
5.	CONCLUSIONS AND RECCOMENDATION	52
5.1	Conclusions	52
5.1.1	Kernel Mode Level	52
5.1.2	User Model Level	52
5.2	Recommendation	53
5.3	Future Work	53
A.	Ransomware Samples	54
B.	Tables	65
	REFERENCES	83

List of Figures

1.1	Ransomware 2013 - 2017 Kaspersky (2017)	12
1.2	Windows Users in Worldwide (Statcounter, 2018)	13