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

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

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

List of Figures