OPEN ACCESS 1

ISSN 2356-5462
http://socj.telkomuniversity.ac.id/ijoict/

Intl. Journal on ICT
Vol. 9, No. 1, Jun 2023. pp. 1-10
doi:10.21108/ijoict.2018.42.203

Comparative Impact Analysis of Ransomware using Dynamic Analysis Techniques on Windows 10

Christopher Arden Anugerah [1], Niken Dwi Wahyu Cahyani [2*], Erwid Musthofa Jadied [3]

[1,2,3]*Informatics Faculty, Telkom University*
Jl. Telekomunikasi. 1, Terusan Buahbatu - Bojongsoang, Telkom University, Sukapura, Kec. Dayeuhkolot, Kabupaten Bandung, Jawa Barat, Indonesia

[*] nikencahyani@telkomuniversity.ac.id

Abstract

Malware, short for malicious software, is software or code specifically designed to damage, disrupt computer systems, or gain unauthorized access to sensitive information. Based on type classification, one of the well-known types of malware is ransomware. Usually, ransomware will encrypt the files on a computer system and then demand a ransom from the owner of the computer system so that the owner can regain access to the encrypted files. Sometimes in some cases, ransomware is able to delete files without input from the computer system owner. This research only uses dynamic analysis approach on the analysis process of three ransomware samples that are known for successfully causing losses to many computer systems throughout the world, namely WannaCry, Locky, and Jigsaw. It utilizes Process Monitor and x64dbg to track the processes carried out by the ransomwares. The purpose of this research is to determine which of the three samples has the highest to lowest damage level using metrics that are based on deletion attack structure and cryptographic attack structure. The findings of this research indicate that WannaCry has the highest damage level followed by Locky and then Jigsaw.

Keywords: cryptographic attack, deletion attack, dynamic analysis, Jigsaw, Locky, malware impact, ransomware, WannaCry

I. INTRODUCTION

Over the past few years, the development of the internet usage has grown drastically. It has affected the way people communicate, money transaction, and also business marketing. All of those sectors are now tied to internet connection to stay relevant [1]. Other than the positive side of internet development, there is also the negative side. People became more creative on building powerful malwares that can target the victim's machine and take control over it remotely. This occurrence made malware attacks more common than before [2], [3], [4].

The goal of malware attacks has expanded to achieve something much more profitable in this modern world, such as money, intelligence, and power [5]. One of malware variants known as ransomware can encrypt victims' files and demand a ransom for their release. This type of malware has had a significant financial impact across various sectors, including healthcare, education, and government. Therefore, an optimal method is needed to

Received on 14 Aug 2020. Revised on 1 July 2020. Accepted and Published on 2 July 2020.