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.

analyze ransomware attacks. By analyzing ransomware attacks, we can understand how ransomware works, what it does, and how to create an effective defense strategy for it. Additionally, it can expose the motives and methods of the attackers, providing valuable information for law enforcement agencies [3], [4]. Detecting ransomware early and preventing it from executing its harmful code is vital to combating these attacks [2].

Complete analysis of ransomware can be difficult and very demanding to do. The time commitment is key to do a very thorough analysis. Not to mention, advanced skills in cybersecurity, programming, and reverse engineering are also essential for a complete analysis towards ransomware. Additionally, the analysis also costs a considerable amount of money for the tools and software licenses. This situation is problematic because ransomware continues to evolve stronger to combat even the most robust protection yet on computers. Thus, it is necessary to find a faster way to analyze ransomware that can give results that are at least almost as accurate as the results obtained from complete ransomware analysis.

One effective method for analyzing ransomware is dynamic analysis. This process is carried out on a virtual machine, ensuring that the infected files are examined in an environment hidden from the ransomware, as some ransomware employs anti-virtual machine and anti-emulator techniques [1]. In dynamic malware analysis, the ransomware is executed in a controlled environment to safely observe its behavior. This analysis utilizes various controlled environments, such as emulators, debuggers, simulators, and virtual machines [2], [5]. By using dynamic analysis approach, we can cutout the time needed for the analysis and lower the cost while still getting accurate results of the impact of ransomware attacks.

The goal of this research is to use dynamic analysis approach to help categorize ransomware based on the impacts of the attack. However, the research is limited only to the Microsoft Windows 10 Operating System and with three samples of ransomware consisting of WannaCry, Locky, and Jigsaw. We use Windows 10 Operating System because it is the most recent major Windows Operating System, making our research more relevant for current and future interests [12]. All three ransomware samples are also chosen because of their popularity in ransomware attacks occurrence [16]. In order to analyze them, we use VirtualBox and analyzing tools such as x64dbg and Process Monitor. VirtualBox is an open-source hypervisor developed by Oracle that is available for many operating systems, x64dbg is a program that observes and examines the execution of other program, and Process Monitor is a monitoring software developed for Windows and Linux [3], [12].

II. LITERATURE REVIEW

A. Malware

Malware or also known as Malicious Software is a software that executes malicious content on computers, cellphones, networks and others. Malware has various types and each type has the same goal, namely affecting the victim's system in various ways such as damaging the targeted system, allowing remote code execution, stealing confidential data, and many more [1]. In total, there are nine types of malware including viruses, RATs, spyware, worms, adware, scareware, bots, ransomware, and cryptominers. Viruses spread harmful code within and between hosts. RATs give attackers remote control. Spyware tracks user activities covertly. Worms replicate and spread through networks. Adware displays unwanted ads. Scareware shows fake alerts to prompt fake antivirus purchases. Bots perform tasks like DDoS attacks. Ransomware encrypts files and demands payment. Cryptominers use resources to mine cryptocurrency [4], [9], [10].

B. Dynamic Analysis

Dynamic analysis involves running code to see how it behaves, making it more effective than static analysis for detecting both known and unknown malware. Techniques include tracking function calls and parameters, pausing execution to examine the state, tracing data flow with data tainting, collecting information from network and memory post-execution, and analyzing physical components' behavior for anomalies. Tools that are usually used in these techniques are TTAnalyze, CWSandbox, Capture, MalTRAK, dAnubis, DynamoRIO, VAMPiRE,