DETECTION AND PREVENTION OF CRYPTO-RANSOMWARE

W.T.M. Chathurya P. Thennakoon

A dissertation submitted in partial fulfilment of the requirement for

Masters of Sciences in Cyber Security and Forensics

Department of Computing

Informatics Institute of Technology, Sri Lanka

in collaboration with

University of Westminster, UK

2021

Abstract

Ransomware attacks has become one of the major cyber scams over the past few years to hit businesses. Specially, attackers getting more advantages from this ongoing pandemic situation for industries such as healthcare, insurance, education, business, finance and government. Ransomware is a form of malicious software which allows hackers to restrict access to a personal's or organizational' s sensitive information within attacks and then demand some form of ransom to lift the information restriction. There are various methods have been suggested to fight against ransomware but it is really hard because of the dynamic behavior of ransomware developers, they always find a method to bypass these fighting methods. There are number of commercial tools available in the market to detect and prevent ransomwares but the accuracy of these tools is bit questionable.

This research is mainly focusing on crypto-ransomware detection. The study was conducted to propose a detection and prevention framework for crypto ransomware. Within this research, two surveys conducted using set of questions with participants using IT professionals and people who are working with digital devices related to different industries. And an experiment was done to review and analyze the behavior of few crypto ransomware attacks and the effectiveness of some of the industry leading tools that have the ability of detection ransomware attacks. The experiment was done using lab environment with the instructions of IT professionals.

After analyzing survey results and results from the experiment, the framework to detect and prevent crypto ransomware was generated. This includes mainly seven steps that helps to maintain the accuracy of the framework. The main aim of the framework is to detect and prevent crypto ransomwares using technologies such as Artificial Intelligence (AI) and Machine Learning (ML) to achieve the highest accuracy.

Keywords: Crypto Ransomware Detection, Detection and Pretension Framework, AI Based ransomware prevention