Universiti Teknologi MARA

Coinminer Malware Detection Using Python Script

Nur Nabilah Binti Muhammad Azlan Jefre

Thesis Submitted in Fulfilment of the Requirement for Bachelor of Computer Science (Hons.) Data Communication and Networking
Faculty of Computer and Mathematical Sciences

July 2020

ACKNOWLEDGEMENT

Alhamdulillah, praises and thanks to Allah because of His Almighty and His utmost blessings, I was able to finish this research within the time duration given.

Firstly, my special thanks go to my helpful and dedicated supervisor, Sir Muhammad Azizi bin Mohd Ariffin for all of his kindness and support during all time and also give me some advices and idea so that I can do well in this project and also solve problem during the project proposal completion. Much obliged to him for his affirmation, supervision, motivation, considerations, proposal and arrangement which led to the completion of this project.

Special appreciation also goes to my beloved parents, my father and my mother who never give up in supporting, pray for me, motivate me, for being my backbone and give motivation so that I can do my best in this project proposal.

Last but not least, I would like to give my gratitude to my dearest friends for helping me and giving me a lot of support and ideas to finish this project proposal. May Allah bless for all of your kindness.

ABSTRACT

The project is about development of CoinMiner Malware Detection using Python. The reason for developing this project is to give enlightenment towards computer users on how to detect coinminer malware. Nowadays coinminer malware has been actively spread among corporate networks. It took over a computer's resources and used them for mining cryptocurrency illegally without a user's permission. Consistently, systems like Bitcoin, Dash, and Litecoin become evermore unified. Moreover, there are also an increasing number of reported cases where malicious coinmining code has been infecting user’s machines for the purpose of illegal mining. Mining has become more of a problem than a solution. Furthermore, users are also unaware that their computer resources have been used for mining which lead to financial loss. This project is needed to give an awareness towards corporate networks about coinminer malware. It is also to suggest Coinminer Malware Detection using Python Script as a new detection method for coinminer malware in a corporate network. The goal of this project is to help the users of corporate networks to detect the coinminer malware and avoid them from being a victim. The limitation and suggestion for future enhancement of this project had been identified based on the analysis of the data collected.

TABLE OF CONTENTS

CONTENT **PAGE**

CHAPTER 1

INTRODUCTION

This chapter provides the background and rationale for the study. Furthermore, this chapter also analyzes the problem statement, objective and scope of this research.

1.1 Background of Study

Coinminer malware is a relatively new term that refers to software programs and malware components created to take over the assets of a computer and use them for cryptocurrency mining without the explicit permission of a consumer. (Stroud, F, 2019). Thus, the computer resources are being obtained illegally by using this malware. Cyber criminals are always searching for new ways of making money, even if the ways they use are illegal. With the rise of digital currencies also known as cryptocurrencies, criminals see a unique way to penetrate an organisation and secretly mine coins through reconfiguring malware.

Hackers have two common ways to get a victim's computer to mine remotely for the cryptocurrencies. One of these is to trick victims into loading their machines with the cryptomining code. This is done through phishing tactics that will give victims a legitimate email encouraging them to click on a link. Once the link has been clicked by the user, the link will immediately run code that places the cryptomining script on the computer. The script then runs in the background as the victim works. (Nadeau, M, 2020)