META-STUDY ON DETECTING ILLICIT CRYPTOCURRENCY MINING

GOVERNMENT RESPONSES TO CRYPTOCURRENCIES' EFFECTS ON CYBERCRIME

An Undergraduate Thesis Portfolio
Presented to the Faculty of the
School of Engineering and Applied Science
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Joseph Davidson

May 9, 2022

SOCIOTECHNICAL SYNTHESIS

Cybersecurity continues to be a critically important aspect in securing and maintaining many of the systems that run our modern economy and world. One of the aspects of cybersecurity that has gained relevance in recent years is the use of cryptocurrencies in a variety of cyberattacks. This technical report focuses on some of the technical methods that have been developed in order to mitigate the negative effects cryptocurrencies are having on cybersecurity systems. Specifically, the technical topic analyzes some of the current means of detecting cryptojacking in the form of a meta-study. The STS research examines how governments are currently responding to the use of cryptocurrencies in crime and cybercrime. In this way, both the technical and the STS topics are seeking to find and analyzes the current tools being used to mitigate some of the negative impacts of cryptocurrencies.

Cryptojacking, which involves the unauthorized use of a device to mine for cryptocurrencies, is one of the ways cryptocurrencies are impacting cybersecurity. The technical portion of this research focuses on this type of malware and current means of detecting it. By researching means of detecting and thereby preventing this illegitimate use for cryptocurrencies, the technical report helps to contribute to mitigating the harmful use of cryptocurrencies. Primarily, this is accomplished by reviewing existing academic work that lays out methods and approaches for detecting cryptojacking. After aggregating these methods, the various aspects (i.e., the strengths and weaknesses) of each of these approaches were analyzed and compared.

The technical report found that there are currently several categories of cryptojacking detection methods. Briefly, the four major ones are: fragment analysis, machine learning methods, web traffic analysis, and behavior-based decision trees. The analysis within the technical report found that each of these methods has relevant use cases. Some of these methods

being better suit for initial detection of novel cryptojacking and others become more useful with larger collections of malware samples. Overall, it was found that the variety of methods are important for a robust system of detection and mitigation.

The STS portion of this research seeks to explore and analyzes current government responses to cryptocurrencies and their impacts on crime and cybercrime. It was found that generally the United States and European Union are taking a regulatory approach, whereas other countries like, China, are banning cryptocurrencies instead. Additionally, the approach a government took in responding to cryptocurrencies' effects on crime could largely be attributed to that government's balance of control and potential economic growth. In order to arrive at these conclusions a variety of sources were used; including: government documents, news articles, and academic papers. In addition to these sources, Actor Network Theory, developed by Latour was used to assist in identifying the motivations behind different government actions.

The US and EU have been taking similar approaches to regulating and enforcing relevant laws around cryptocurrencies. Much of the information on what these governments are doing came from official government reports published by the Department of Justice and the European Securities and Markets Authority. In both cases the US and the EU have also stated in various ways that they want to allow cryptocurrencies and the surrounding technologies to develop while also eliminating the negative aspects of them.

While cryptocurrencies are relatively new, that has not prevented them from having harmful impacts on cybersecurity and crime in general. These negative effects are starting to be mitigated, both by detecting cryptojacking and through government regulations and enforcement. It will continue to be important in the coming years for technical, as well as social and political means of mitigating cryptocurrencies' negative impacts are pursued and implemented.

TABLE OF CONTENTS