COMMIT MALWARE ANALYZER: DETECTING MALICIOUS SOFTWARE THROUGH SEMANTIC ANALYSIS OF MALICIOUS SOFTWARE DEVELOPERS' BEHAVIORS, DESCRIPTIVE ATTRIBUTES, AND CODE PUBLICATIONS

DEFINING ETHICAL IMPLICATIONS IN MALWARE INTERACTION WITHIN THE CYBERSECURITY PROFESSION

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

Vanessa Barlow

May 6, 2021

SOCIOTECHNICAL SYNTHESIS

The cybersecurity community mitigates and responds to cyber threats by conducting malware analysis and detection research that requires them to work alongside malware. The technical research aims to diminish cyber threats by building a tool to identify malware. More specifically, the tool distinguishes malicious software developers on the well-known, software developer platform, GitHub. To do so, interacting with malware was essential to the project. The STS research analyzes the methods, ethics, and effects of cybersecurity professionals working in conjunction with malware. This analysis is imperative because many cybersecurity projects, including the technical research, rely on interacting with malware. Thus, when dealing with dangerous data, there must be assurance that cybersecurity professionals are performing their occupational duties with an iterative, ethical process. The tightly coupled STS research addresses this issue in response to the technical research, but more broadly, to all cybersecurity projects.

The technical research is a novel approach that identifies malicious users on GitHub to prevent the sharing of vulnerable or dangerous code in the computing community. The tool consists of a machine learning model that receives software, analyzes the software, and distinguishes whether the software is safe or contains malware. Additionally, the technical project contributes contemporary methods for GitHub data collection which is essential for this project and future projects that focus on code sharing platforms. Results indicated that the tool performed as well as a comparable state-of-the-art tool on various performance levels. However, the tool would seldomly misidentify a malicious GitHub user, which concluded that the tool needs further fine tuning and malware samples to identify different types of malware. Overall, the tool was successful for the scope of the project, but can be improved for future use.

The STS research focuses on analyzing the implementation of ethical guidelines when cybersecurity experts interact with malware and the subsequent impact of the associated ethical dilemmas. To analyze this question, the Actor-Network Theory (ANT) was used to model three core actants of the cybersecurity profession: ethical guidelines, malware interaction, and the relationship to a criminal hacker. To delve into these actants, ethical literature from cybersecurity experts, researchers, philosophers, and engineers responsible for crafting ethical guidelines were employed to form the main argument for this research.

Through this research, it was shown that cybersecurity professionals tend to perform unethical behaviors that contradict ethical guidelines to fulfill an ethical duty. To identify unethical behaviors, routine malware interaction duties, such as malware analysis, disassembly, reconstruction, and counteraction, were researched and behaviors that directly violated the Association of Computing and Machinery (ACM) code of ethics were outlined. Furthermore, the research extended to highlight the implications of performing unethical behaviors to achieve an ethical obligation. Research claimed that performing unethical behaviors in regards to malware may affect the morality and judgment of a cybersecurity professional. This potential effect was also found to contradict the ACM code of ethics. A solution to incorporate ethical reflections as an iterative process was produced to minimize unethical behaviors and the potential effects on cybersecurity professionals. The solution consisted of constructing an ethical organization with direct, technical representatives attached to each cybersecurity team within a company. The goal of the ethical representative is to comprehend the actions performed by the cybersecurity team as they oversee and engage the team in an ethical discussion about their actions.

The technical and STS research both pose solutions to overcome a crucial challenge in the cybersecurity community: the challenge to implement novel methods to secure software

infrastructure while reasoning and behaving ethically. The technical project responds to this dilemma by providing a novel approach to reduce the amount of malware readily available on code sharing platforms. Furthermore, the STS research forms a solution to promote ethical behaviors for cybersecurity professionals while interacting with malware.

TABLE OF CONTENTS