DEFINING ETHICAL IMPLICATIONS IN MALWARE INTERACTION WITHIN THE CYBERSECURITY PROFESSION

A Research Paper submitted to the Department of Engineering and Society
In Partial Fulfillment of the Requirements for the Degree
Bachelor of Science in Computer Science

By

Vanessa Barlow

March 25, 2021

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

ADVISOR
Catherine D. Baritaud, Department of Engineering and Society

Cyber threats arise from malware, “a set of instructions that run on your computer and make your system do something that an attacker wants it to do” (Skoudis, 2003, “Defining the Problem”). The cybersecurity community constantly conducts malware analysis and detection research to minimize cyber threats and vulnerabilities. Cyber threat research and analysis is essential since new and improved cyber-attacks are created each day, and professionals need to know the latest cyber-attacks and threats to mitigate them.

Although the advancement in computing technology has produced crucial benefits across industries, it has also contributed to innovative, large-scale cyber-attacks. For example, the U.S. witnessed a 600% increase in federal cyber incidents between 2006 and 2016, coining the attacks as the “cyber Pearl Harbor” to highlight the gravity of cyber incidents (Karim, 2020, p. 1). Additionally, data from 2018 reported a 44.7% spike in U.S. data breaches with 73% of U.S. businesses experiencing a cyber breach (Kennerly, 2018, p. 123). Looking forward, assessments from hackers, cybersecurity researchers, and information security professionals suggest that 11 major industries are highly vulnerable to future cyber threats due to advanced cyber technology. The industries addressed include: implanted medical devices, telework, smart-home devices, autonomous vehicles, cities, trains, aviation technology, 5G networks, schools, hospitals, and energy grids (Kamping-Carder, 2020, Section 2, paras. 2-16). Furthermore, the acknowledgement of current and future cyber-attacks has challenged cybersecurity experts to implement novel methods to secure software infrastructure while reasoning and behaving ethically.

The technical research responds to this challenge by building a malware detection tool to classify malicious users on GitHub, an online software development community. The tool

classifies GitHub users based on a developer's code contribution to the development community. If the tool identifies malware on a specific GitHub user's account, then that user is labeled as malicious. Malware is essential to the technical research since it is used to train and test the tool's classification model. Therefore, it is critical for researchers to interact with malware to successfully construct the tool. Thus, the tightly coupled STS research explores the ethics of cybersecurity experts who manage malware in fulfillment of their occupational role.

The STS research aims to gain insight on the implementation of ethical guidelines as cybersecurity experts interact with malware and the impact of associated ethical dilemmas. To analyze this question, the Actor-Network Theory (ANT) proposed by Latour (1992), and Law and Callon (1988), will be used to model three core actants of the cybersecurity profession: ethical guidelines, malware interaction, and the relationship to a criminal hacker. This framework is used to identify where moral dilemmas occur in the malware interaction process and where ethical guidelines fail to address moral conflicts. A solution that integrates ethical guidelines in the malware interaction process will be proposed to minimize instances of unethical behavior that transpire in the fulfillment of an ethical duty.

IS MALWARE INTERACTION IN THE CYBERSECURITY PROFESSION A PROBLEM?

There are two prominent interpretations of the cybersecurity profession. The first view showcases the group in a positive light, where cybersecurity experts are seen as "white hat 'hackers'" who try "to thwart [cybercriminals]" (Dadkhah, Lazian, & Borchardt, 2018, "Problems Faced in Discovering These Fraudulent Methods," para. 3). The second view highlights the profession in a skeptical way, viewing cybersecurity experts as potentially malicious actors since they must "think like hackers to analyze their methods" (Dadkhah et al,

2018, Introduction," para. 6). A group of cybersecurity researchers, Dadkhah et al. (2018), recognize these opposing viewpoints and distinguish cybersecurity professionals from the typical criminal hacker to reinforce the idea of cybersecurity experts as white hat hackers. They argue seven main differences: 1.) experts analyze current attacks while hackers launch new attacks; 2.) experts test on simulated systems while hackers attack live systems; 3.) experts acquire permission for unauthorized use while hackers perform illegal activities to bypass permissions; 4.) experts work closely with software developers while hackers conceal their techniques; 5.) experts disclose their identity while hackers remain anonymous; 6.) experts prioritize protecting the integrity of science while hackers employ their techniques for self-gain; and 7.) experts share their work publicly while hackers hide details related to their attacks ("Problems Faced in Discovering These Fraudulent Methods," para. 3). These distinctions reinforce how cybersecurity experts value protecting and preserving the integrity of systems and refuse to take part in criminal hacker activity, strengthening the positive view of the cybersecurity profession.

Although Dadkhah et al. (2018) defend cybersecurity professionals, like themselves, as white hat hackers, they also propose an idea that supports the second outlook of cybersecurity professionals. They state that due to the complicated nature of cyber-attacks, cybersecurity experts must reason as criminal hackers to understand cybercrime methods and reverse engineer cyber-attacks to detect and defend against them ("Introduction," para. 6). This change in mentality is problematic since it leads to immoral and unethical reasoning and ultimately is the cause of skepticism regarding the cybersecurity profession.

Cyber threat researcher, Pompon (2018), addresses that immoral and unethical reasoning within the cybersecurity profession is a "growing problem and one that not enough people are

talking about" (para. 15). He details how cyber professionals who are regularly exposed to malware search the dark web, disassemble malware, and create malware to counteract hackers (para. 1). Pompon claims that these professionals tend to "find themselves using stealth, misdirection, and even outright deception" in their profession as well as in their personal life (para. 2). His experience in the field directly contradicts the distinction between hackers and cybersecurity researchers that Dadkhah et al. (2018) asserts and supports the idea that unethical reasoning is an issue in the cybersecurity profession.

This notion challenges the moral codes within the cybersecurity community since cybersecurity experts may fulfill ethical responsibilities by using unethical measures. Furthermore, the objective of this research is to understand where ethical guidelines fail during the malware interaction process and how failing to reason ethically could affect the cybersecurity expert. To fully comprehend the ethical implications of malware interaction in a professional setting, an in-depth analysis of the current ethical guidelines and relationship between hackers and cybersecurity experts must be conducted alongside the malware interaction process.

THE CYBERSECURITY PROFESSION: ETHICAL GUIDELINES, MALWARE INTERACTION, AND RELATIONSHIP TO THE CRIMINAL HACKER

The Actor-Network Theory (ANT) will be used to model the cybersecurity profession with regards to ethical guidelines followed in the field, malware interaction within the occupation, and relationship to the hacker as shown in Figure 1 on page 5. All actants in Figure 1 play a role in the cybersecurity profession. Ethical guidelines outline the behaviors and obligations that cybersecurity experts should adhere to; malware interaction represents the cybersecurity expert's occupational role when counteracting hackers, analyzing, disassembling,

and reverse engineering malware; the relationship to a criminal hacker constitutes the hacker mindset that cybersecurity experts embody when interacting with malware, as well as the similarities in technical competence and differences in occupational goals.

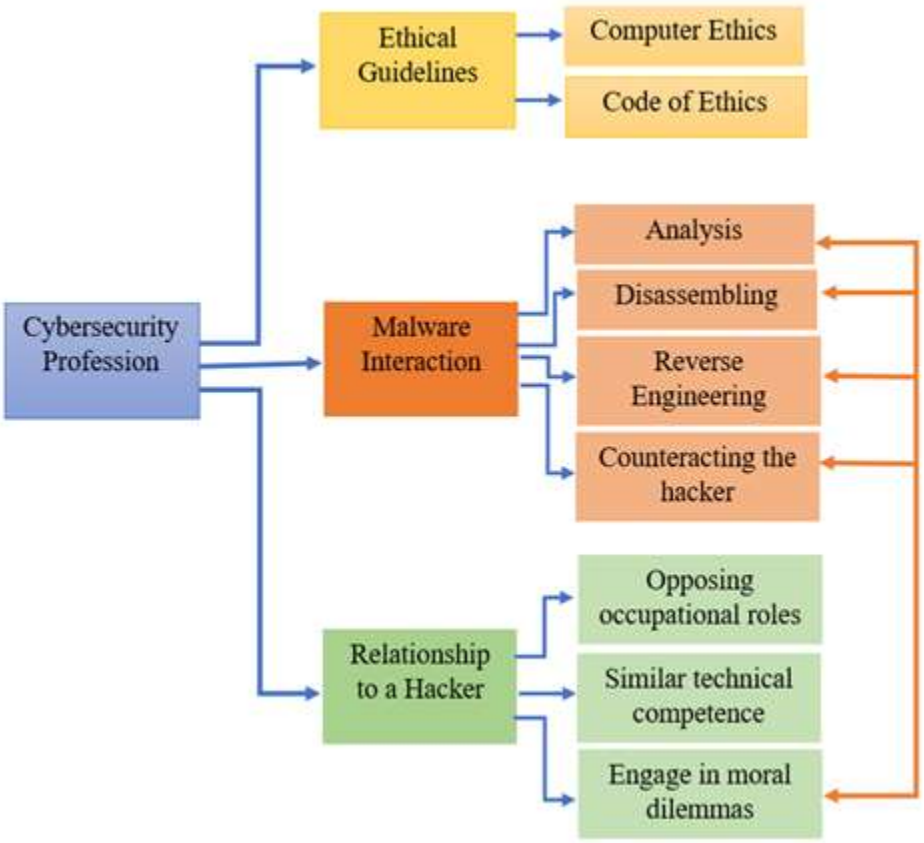

Figure 1: Flow Diagram Outlining the Cybersecurity Profession and the Moral Dilemma Challenges in Malware Interaction. This diagram visualizes three prominent actants in the cybersecurity profession: ethical guidelines, malware interaction, and relationship to the typical criminal hacker. There is emphasis between malware interaction and engaging in moral dilemmas as the STS research will explore the moral dilemmas that occur when interacting with malware (Adapted by Barlow (2020) from Carlson, 2007).

As shown in Figure 1, there is a linkage between engaging in moral dilemmas and core components of the malware interaction role. Both the criminal hacker and cybersecurity professional engage in moral dilemmas, however, the difference is that the professional may not

completely comprehend that they are participating in unethical conduct when working with malware. To understand why cybersecurity experts resort to unethical practices within the course of malware interaction, an ethical analysis of each actant must be conducted.

Figure 2 delves further into the connection between malware interaction and the ethical dilemmas faced by cybersecurity professionals. As illustrated, examples of unethical practices

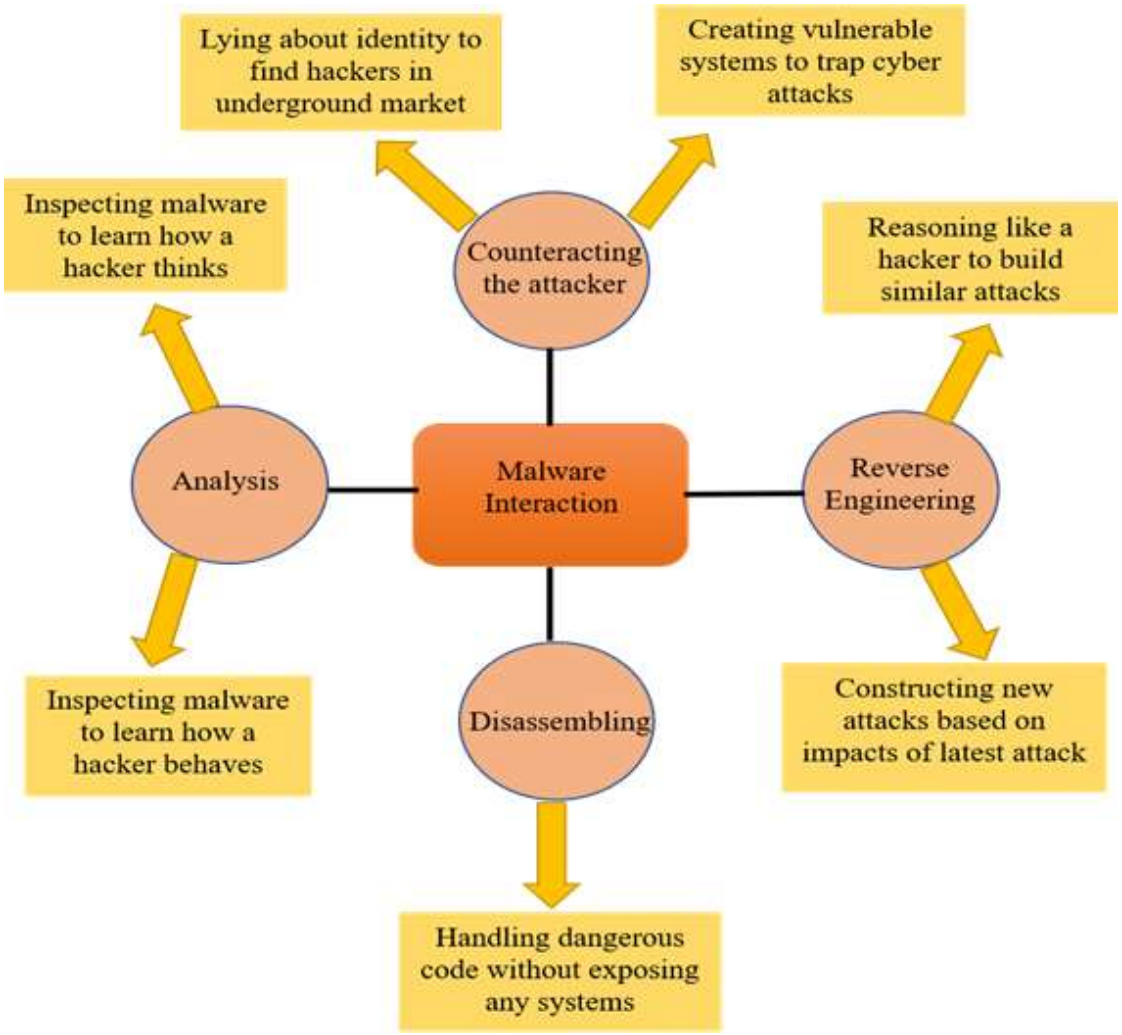

Figure 2: Moral Dilemmas Faced in the Malware Interaction Process of the Cybersecurity Profession. This diagram visualizes moral and ethical dilemmas witnessed by cybersecurity professionals when interacting with malware. (Adapted by Barlow (2020) from Carlson, 2007)

during malware interaction are identified. For instance, when counteracting a hacker, a cybersecurity expert may enter the underground malware market and pretend to be a criminal hacker to gain knowledge on the malware and method employed by hackers. Likewise, the expert may also set up vulnerable systems to attract hackers in hopes of receiving more information about the malware the hacker uses. Both actions end in fulfilling an ethical obligation since the cybersecurity expert uses knowledge about the malware to defend against the hacker. However, the means to accomplish these tasks involve lying and intentionally creating insecure systems which are indeed ethical concerns. Similar issues are recognized in the analysis, disassembly, and reverse engineering roles when interacting with malware. To further comprehend why these unethical practices occur, a discussion of the limitations of ethical guidelines in regards to malware interaction is necessary.

THE LIMITATIONS OF THE COMPUTER SECURITY CODE OF ETHICS

Computer security ethics are overarching guidelines that aid computer security professionals to practice their skills ethically. Most security professionals adhere to the Association for Computing Machinery (ACM) code of ethics. These guidelines were revised for the first time in 2018 to "reflect the values of the computing profession in a way that can help ACM members make appropriate ethical decisions" (Gotterbarn et al., 2018, p. 122). One of the most important revisions involved clarifying the difference between "must" and "should". There are three instances in the ACM code of ethics where the word "must" is used and requires computing professionals to adhere to the guidelines "even when a course of action is ethically justified" (p. 123). The three uses of "must" requires computing professionals to support public safety and well-being, and obey laws or regulations imposed by the government and the organization for which they work. The word "should" is used 76 times and is stated to provide

professionals with the "opportunity to articulate their analysis and be transparent about their ethical reasoning" (p. 123). Thus, the ACM code of ethics supports professionals to freely exercise ethically justified actions if they do not oppose government and company regulations nor inflict harm on society. The freedom in decision making supported by the ACM code of ethics is reasonable since moral conflicts arise and vary by situation, but it requires professionals to reason ethically throughout their behaviors.

Reasoning ethically seems like an innate ability, however, computing experts develop a binary reasoning, which is reinforced by their education with computer technology, that can ultimately impact ethical decision making. Woolgar and Russell (1990) reaffirm that computer education instills binary logic within decision making since "the binary logic of computer technology is vivid in its contrasts between 'working' and 'not working': on/off; zero/one; right/wrong" (p. 34). Simply, the binary mentality categorizes actions as right or wrong (Woolgar & Russell, 1990, p. 34). An example of the application of the binary mentality in the cybersecurity profession can be shown through a cyber incident at Bank of America. A Bank of America employee destroyed data by injecting malware into Bank of America's computer network. Although he injected malicious software into his company's computer system, which is an unethical act, he justified his actions since he did not commit a crime, steal information, nor break any rules, reinforcing the idea of binary logic within decision making (Taylor, 1999, p. 138).

Ethical guidelines do not only fail during the malware interaction process because of the binary mentality, but also because computer scientists tend to "judge actions in terms of result, or based on actual damages" (Taylor, 1999, p. 139). This perspective implies that actions and

behaviors tend to be evaluated by the end results as opposed to applying ethical guidelines iteratively throughout a project. Additionally, Taylor (1999) details the ill-defined implementation of ethics within the cybersecurity profession since there are disputes on correct ethical procedures (p. 139). This internal conflict can contribute to neglecting certain ethical guidelines throughout the course of a cybersecurity expert's work.

Furthermore, computer security ethical guidelines serve to promote ethical and moral reasoning rather than enforcing ethical decision making. The ACM code of ethics only succeeds if the cybersecurity expert can reason ethically and thoroughly apply ethical principles throughout their occupational role. As suggested, common pitfalls arise when binary logic is applied in decision making and when ethical guidelines are neglected during the process of any given task. To gain a deeper understanding of the tasks assigned to cybersecurity experts and the ethical dilemmas they face during them, there must be a review of malware interaction in the cybersecurity profession.

MALWARE INTERACTION IN THE CYBERSECURITY PROFESSION

As illustrated in Figure 2 on page 6, malware interaction in the cybersecurity profession is composed of four primary obligations: counteracting the hacker, malware analysis, malware disassembly, and reverse-engineering. Most organizations have a malware response team to accomplish these tasks. Mohanta and Saldanha (2020) use the term "malware hunters" to describe cybersecurity professionals who actively search and defend against potential cyber threats. Much of their work is devoted to being up-to-date on the latest cyber-attacks and informing the cybersecurity community on new malware trends and attacks ("The Combat Teams," para. 9)". However, some malware hunter practices are morally ambiguous.

For example, malware hunters construct honeypots to attract cyber-attacks to learn about the criminal hacker's methods and logic. A honeypot is a term for a computer system that is "intentionally made vulnerable and easily accessible to attract malware and other attackers" (Mohanta &Saldanha, 2020, "The Combat Teams," para. 6). According to Principle 2.9 of the ACM code of ethics, computing professionals have a "responsibility to ensure that the systems they create are secure" (Gotterbarn et al., 2018, p.123). Thus, intentionally constructing vulnerable systems is an unethical practice. Nevertheless, information retrieved from a honeypot can be pertinent in building secure defenses against similar attacks. Therefore, cybersecurity experts justify the creation of a honeypot due to the ethical outcome they achieve.

Another controversial practice is the impersonation of criminal hackers by cybersecurity experts in order to withdraw information from malicious actors in the underground market. Part of impersonating a criminal hacker involves forging one's identity, sharing information with other malicious actors, gaining criminal hackers' trust, and a variety of other malicious activities (Mohanta & Saldanha, 2020,"The Combat Teams," para. 9). Principle 1.3 of the ACM code of ethics urges computing professionals to "be honest and trustworthy" (Gotterbarn et al., 2018, p. 125). Lying and engaging in immoral activities violates this principle. However, the cybersecurity expert receives information that may be substantial to their work. Therefore, since the unethical actions compose an ethical task, cybersecurity professionals justify these behaviors.

Dissecting, analyzing, and reverse engineering malware are roles that work together "to obtain information on the functionality of the malware, information on the attacker, and Indicators of Compromise (IoC)" (Mohanta & Saldanha, 2020, "The Combat Teams," para. 12). At first glance, these actions do not seem problematic. However, Sullins (2014), a Ph.D. philosopher who focuses on engineering and computer ethics, believes that "working with

malware is not ethically neutral" (p. 2). In fact, during the process of disassembling, analyzing and reconstructing malware, cybersecurity professionals embody the aforementioned hacker mentality. The hacker mentality affects one's ability to reason and behave morally. If a person programs themselves to "to think immorally, then one might lose the ability to make good choices" (Sullins, 2014, p. 2). Thus, cybersecurity experts who interact with malware must develop the difficult technique of "compartmentalizing their ability to think nefariously so that it does not overtake their ability to reason morally" (Sullins, 2014, p. 2). The possible repercussions from engaging in the hacker mentality correlates to Principle 1.2 of the ACM code of ethics to avoid harm, where harm is defined as any "negative consequences to any stakeholder" which includes unjustified mental injury to the computing professional (Gotterbarn et al., 2018, p. 124). However, this principle is overlooked since harm is rarely considered to apply to the professional who performs the task that may cause harm and since an ethical obligation is completed in the process: the cybersecurity expert gains the information needed to secure systems and defend against criminal hackers.

As outlined, malware interaction presents ethical dilemmas to cybersecurity experts routinely. However, if unethical actions can fulfill an ethical obligation, then the actions are usually considered justified. Moreover, another question of this research is to understand what ethical implications arise due to the engagement of unethical practices. To resolve this question, the relationship between a criminal hacker and a cybersecurity expert will be explored.

RELATIONSHIP TO THE TYPICAL CRIMINAL HACKER

Criminal hackers and cybersecurity experts have distinctly different occupational roles as noted by Dadkhah et al. (2018) earlier in this paper. Yet, despite these differences, they do share

commonalities. For instance, both hackers and cybersecurity experts share “patience and the ability to reason through logic problems” (as cited in Chua & Holt, 2016, “Hacking Behaviors and Techniques of Neutralization, para. 4). Furthermore, hackers and cybersecurity professionals share some other subtle similarities.

In a criminal hacker mindset study conducted by Chua & Holt (2016), hacker motivations were analyzed and predicted through a theory called the neutralization framework. This framework found that hackers typically “rationalize their actions or neutralize a sense of guilt and responsibility” prior to distributing or creating malware (“Hacking Behaviors and Techniques of Neutralization, para. 5). This rationalization process allows them to think of their actions as justified and benevolent. A similar rationalization process is used within the cybersecurity profession since cybersecurity experts rationalize unethical behavior and reasoning since they lead to an ethical and acceptable product. Another result of the study concluded that criminal hackers tend to participate in unethical behaviors when they believe that “hacking does not cause harm or actually benefits society” (“Discussion and Conclusion”, para. 6). This abides by the ACM code of ethics’ principles to avoid harm and hold the public well-being paramount (Gotterbarn et al., 2018). Likewise, cybersecurity experts justify their unethical actions similarly since they perform unethical actions to achieve outcomes that will protect society from cyber breaches and cyber-attacks.

The hacker mindset and cybersecurity expert mindset are very similar, which is logical since cybersecurity experts must develop a hacker mentality when performing unethical actions in hopes of creating an ethical outcome. Referring to Sullins (2014), developing this type of nefarious mentality could be detrimental to the cybersecurity expert’s moral reasoning since moral reasoning is a skill that is developed over time. Thus, the impairment of moral reasoning is

the most significant ethical implication that can occur through implementing unethical actions while performing an ethical task. Moreover, other implications, such as passing down unethical procedures to younger generations of cybersecurity professionals, can occur and negatively impact the future generations of cybersecurity professionals.

Furthermore, an important question is raised: Is a cybersecurity expert a hacker if they share subtle similarities with a criminal hacker? The answer, of course, is no. Their occupational role differs as clearly outlined by Dadkhah et al. (2018). The commonalities highlighted in this section do not imply that cybersecurity experts are hackers. In fact, they emphasize the unawareness and ignorance of the unethical actions used to achieve ethical outcomes within the cybersecurity community. The next section will provide some ideas on how to combat ethical dilemmas within the malware interaction process to reduce the extent of the ethical implications that were discussed in this section.

HOW TO INTEGRATE ETHICS IN THE MALWARE INTERACTION PROCESS

As highlighted in this paper, the ACM code of ethics act as a guide rather than a law for computing professionals to follow. The ACM code of the ethics is constructed in this way for various reasons, but mainly because there are a vast number of different scenarios that require computing professionals to ethically reason through. Therefore, the solution to integrate ethical guidelines through the malware interaction will consist of: implementing an ethical organization with direct representatives attached to each cybersecurity team within a company, mandatory malware ethical courses, and a guideline that resorts to an unethical option if it is truly necessary. Figure 3 describes how the ethical representative will be involved when cybersecurity professionals engage with malware.

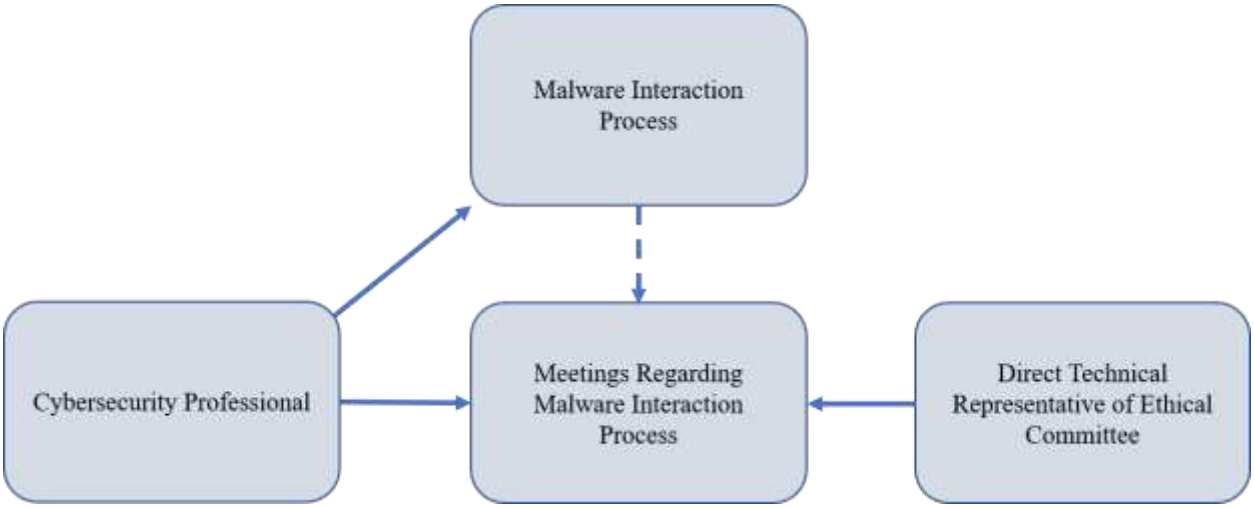

Figure 3: Solution to Integrate Ethics during the Malware Interaction Process. This diagram illustrates how a technical representative from an ethical committee will attend meetings to discuss the actions that a cybersecurity professional performed when interacting with malware. (Adapted by Barlow (2020) from Carlson, 2007)

First, there must be an ethical committee within an organization that employs cybersecurity professionals. Then, there will be a direct representative from this committee who is technically competent and can understand the malware interaction process. This representative will attend meetings based on the frequency that cybersecurity professionals interact with malware and the frequency of cybersecurity team meetings. As illustrated in Figure 3, the representative from the ethical committee is not directly involved in the malware interaction process. Thus, cybersecurity experts must thoroughly note their actions and report their actions honestly during the direct meeting with the technical representative. The representative will serve as a resource for ethical reasoning. Their duties will consist of fully understanding the actions performed by the cybersecurity team and engaging the cybersecurity team in an ethical discussion about their actions.

Furthermore, the cybersecurity profession needs to make concrete changes within their teams and organizations. The solution proposed above will give cybersecurity professionals the opportunity to take part in ethical discussions about their work and allow for reflection on the justification of their actions. However, each organization should instill mandatory ethics courses to discuss hypothetical situations that cybersecurity professionals may run into in the future, and enforce the rule of only incorporating unethical actions when it is truly necessary.

In brief, this thesis addresses the problem of justifying unethical actions to produce ethical outcomes in the malware interaction process. The most significant implication of these unethical practices is the potential to gradually affect the moral reasoning a cybersecurity professional develops overtime. This complication was outlined through the Actor-Network Theory (ANT) to frame how the problem resides in the malware interaction process and how ethical guidelines are overlooked in this setting. Additionally, a comparison of criminal hackers and cybersecurity professionals was conducted to showcase the similarities in the rationale behind behaving and reasoning unethically. Moreover, a solution consisting of integrating a representative of an ethical committee to oversee the behaviors and reasonings of cybersecurity teams was described to combat unethical actions and implications in the malware interaction process. This solution will not eliminate unethical actions throughout the profession, but it is a solution that will allow for cybersecurity professionals to reflect on their implementation of ethics across the span of their work. Ethical reflections can generate positive improvements within the profession since future generations of cybersecurity professionals will be more aware of ethical dilemmas and confrontations they may perceive. To eliminate unethical actions within the cybersecurity community, more research must be conducted on the most strategic way of impacting a cybersecurity professional's decision making. A potential solution could include

editing the ACM code of ethics or possibly creating new rules or regulations. Regardless, the elimination of unethical actions within the cybersecurity community is out of scope for this particular research and would need further research to solve.

WORKS CITED

Barlow, V. (2020). *Flow Diagram Outlining the Cybersecurity Profession and the Moral Dilemma Challenges in Malware Interaction.* [Figure 1]. *STS Research Paper: Defining Ethical Implications In Malware Interaction within the Cybersecurity Profession* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Barlow, V. (2020). *Moral Dilemmas Faced in the Malware Interaction Process of the Cybersecurity Profession.* [Figure 2]. *STS Research Paper: Defining Ethical Implications In Malware Interaction within the Cybersecurity Profession* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Barlow, V. (2020). *Solution to Integrate Ethics during the Malware Interaction Process*. [Figure 3]. *STS Research Paper: Defining Ethical Implications In Malware Interaction within the Cybersecurity Profession* (Unpublished undergraduate thesis). School of Engineering and Applied Science, University of Virginia. Charlottesville, VA.

Dadkhah, M., Lagzian, M., & Borchardt, G. (2018). Academic information security researchers: Hackers or specialists?. *Science & Engineering Ethics, 24*(2), 785-790. doi: 10.1007 /s11948-017-9907-1

Gotterbarn, D., Bruckman, A., Flick, C., Miller, K., & Wolf, M. J. (2018). ACM code of ethics: A guide for positive Action. *Communications of the ACM, 61*(1), 121-128. doi: 10.1145 /3173016

Kamping-Carder, L. (2020, October, 9). The future of everything: The cybersecurity issue --- Hacking's next targets: Systems we use everyday may not be secure tomorrow. Here's what cybersecurity experts say could be a future focus for attacks. *The Wall Street Journal,* Retrieved from https://www.wsj.com/

Karaim, R. (2020). Cyberwarfare. CQ Researcher, 30(9), 1-55. Retrieved from http://library .cqpress.com/

Kennerly, E. (2018). Privacy and the internet. CQ Researcher, 28(6), 121-144. Retrieved from http://library.cqpress.com/

Latour, B. (1992). Where are the missing masses? The sociology of a few mundane artifacts. In

W. Bijker & J. Law (Eds.), *Shaping technology, building society: Studies in sociotechnical change* (pp. 225-258). Cambridge, MA: MIT Press.

Law, J. & Callon, M. (1988). Engineering and sociology in a military aircraft project: A network analysis of technological change. *Social Problems, 35*(3), 284-297. doi:10.2307/800623

Martin, M. W. & Schinzinger, R. (2010). *Introduction to engineering ethics* (2nd ed.). New York, NY: McGraw-Hill.

Mohanta A. & Saldanha, A. (2020). *Malware analysis and detection engineering: A comprehensive approach to detect and analyze modern malware.* Retrieved from https://learning.oreilly.com/

Pompon, R. (2018, May). The ethical and legal dilemmas of threat researchers. *(IN)SECUREMagazine.* Retrieved from https://www.helpnetsecurity.com/

Skoudis, E., & Zeltser, L. (2003). *Malware: Fighting malicious code.* Retrieved from https://learning.oreilly.com/

Taylor, P. A. (1999). *Hackers.* Oxfordshire, UK: Taylor & Francis Ltd / Books.

Woolgar, S. & Russell, G. (1990). *The social basis of computer viruses*. Retrieved from:

https://ieeexplore.ieee.org/xpl/conhome/1813/proceeding