Malware Analyst Career

Berline Gabriel

Old Dominion University

CYSE 201s

Bora Aslan

April 13, 2025

Malware Analyst Career

Introduction

With the emergence of digital social platforms where people interact and communicate with each other through texts, images, videos, or audio, the rise of online cybercrimes is aimed at taking advantage of not just individuals but collectives. Researchers and social analysts began to try to understand the digital world, interpreting the way in which individuals who were digitally and socially connected could be manipulated which lays out a foundation for social science research in the world of cybersecurity (Carley, 2020). Social science disciplines, such as criminology, sociology, psychology, and political science, can be necessary for this career. The role of social science research remains critical, especially for the career of malware analysts who are responsible for examining malicious software to understand the structure, behavior, and potential impact of such software on end users. This paper describes how malware analysts require and depend on social science research and how their career contributes to protecting marginalized groups and society.

Behavioral Psychology in Malware Analysis

Understanding human motivation and behavior is the key principle of social science research, which helps malware analysts recognize how different forms of malware, including phishing attacks, ransomware, or social engineering tactics, manipulate emotions like urgency or fear to mislead users of the systems (Rains, 2020). The malware created to manipulate and trick users, such as a social engineering tactic, requires the malware analyst to understand which linguistic strings are most effective in triggering the response of the user to anticipate what groups are most vulnerable who might be affected by the malware. From a social science research perspective, this application of behavioral psychology helps malware analysts

contribute to the broader societal objective of achieving equality and equity in technology to develop more just and inclusive policies.

Sociocultural and Targeted Threats

Underrepresented individuals often have limited access to cybersecurity awareness which requires programs and security tools that are culturally relevant and accessible to marginalized communities in order to ensure that protection is inclusive. In collaboration with social science research, malware analysts help develop security tools that protect poor and marginalized communities while taking into account human behavior to safeguard them from malware attacks. The research principles of social science help malware analysts assess not only how malware works but also the reason to demonstrate who it seeks to harm and why it is created. This supports the ethical responsibility that malware analysts must carry which connects to the social science research, guiding analysts in making informed decisions and developing more effective policies and strategies to balance security needs with individual privacy rights.

Ethical Responsibility in Malware Analysis

Ethics play a significant role in social science principles and research to help analysts navigate complex ethical dilemmas and guide ethical decisions about user privacy, responsible disclosure, and how threat intelligence is shared, involving principles of social responsibility and moral reasoning (Cobb & Lee, 2014). In the context of ethics in social science research, analysts must weigh the urgency of responsible disclosure while analyzing malware that affects any system to prevent potential widespread panic. By understanding human behavior and ensuring ethical principles, integrating social science research in cybersecurity becomes even more critical and effective in ensuring inclusive and ethical practices that protect all members of society.

Conclusion

Therefore, malware analysts can perform effectively with insights from social science principles and research while being socially sensitive and culturally aware to protect marginalized groups and make ethical decisions. This multidisciplinary work requires malware analysts to collaborate across departments and in the daily routine of individuals to effectively interpret the intent behind cyber threats and understand attacker motivations to contribute to more countermeasures. Thus, social science and principles are essential in the daily routines of malware analysts to ensure a safer and more equitable digital world.

References

Bhattacherjee, A. (2012). *Social science Research: principles, methods, and practices*. Digital Commons @ University of South Florida.

Carley, K. M. (2020). Social cybersecurity: An emerging science. *Computational and Mathematical Organization Theory, 26*(4), 365–381.

Cobb, S., & Lee, A. (2014). Malware is called malicious for a reason: The risks of weaponizing code. *2014 6th International Conference on Cyber Conflict (CyCon 2014)*, 71–84.

Rains, T. (2020). *Cybersecurity Threats, Malware Trends, and Strategies: Learn to mitigate exploits, malware, phishing, and other social engineering attacks*. Packt Publishing Ltd.