Dissecting ATM Malware as a Digital Forensics Investigator

William S. Matos Díaz

Old Dominion University

wmato002@odu.edu

Abstract

Automated teller machines (ATMs) are computer systems designed to manage bank funds. These computers are considered prime targets for criminals due to their ability to hold significant amounts of cash and are vulnerable to on-site and remote attacks. For digital forensic investigators, it is critical to understand the types of exploits these machines are susceptible to, as they provide an excellent source of evidence. To effectively analyze ATM attacks, investigators must be familiar with how ATMs operate, the underlying operating system architecture, the various attack vectors used by criminals, and the techniques employed to steal assets. Utilizing Secondary Data Analysis / Bibliographic research, this investigation aims to highlight the importance of awareness of ATM attacks in the digital forensic industry and outline the proper process to follow when analyzing such attacks. Additionally, investigators should be knowledgeable about the countermeasures used to prevent such attacks, enabling them to identify any areas of vulnerability that were exploited by the criminals. By understanding the intricacies of ATM attacks and their potential impact on society, digital forensic investigators can improve their ability to collect and analyze evidence effectively.

References

Harper, A., Regalado, D., Linn, R., Sims, S., Spasojevic, B., Martinez, L., Baucom, M., Eagle, C., & Harris, S. (2018). Gray Hat Hacking: The Ethical Hacker's Handbook, Fifth Edition (5th ed.). McGraw Hill.

2 Editors: [To be filled later]

Hsieh, M-L. & Wang, S.Y.K. (2018). Routine activities in a virtual space: A Taiwanese case of an ATM hacking spree. International Journal of Cyber Criminology, 12(1), 333-352. doi: 10.5281/zenodo.495776

Kasanda, E. and Phiri, J. (2018) ATM Security: A Case Study of Emerging Threats. International Journal of Advanced Studies in Computers, Science and Engineering. https://www.researchgate.net/publication/330133482_ATM_Security_A_case_study_of_Emerging_Threats

NCR Corporation. (2017). ATM SECURITY Explaining Attack Vectors, Defense Strategies and Solutions. NCR. Retrieved October 4, 2022, from https://www.ncr.com/content/dam/ncrcom/content-type/brochures/ATM_Security_white-paper-attack-vectors-and-solutions.pdf

Trend Micro Incorporated. (2017). Cashing in on ATM Malware A Comprehensive Look at Various Attack Types. Trend Micro. Retrieved October 6, 2022, from https://documents.trendmicro.com/assets/white_papers/wp-cashing-in-on-atm-malware.pdf