Detection of Fileless Malware through Network Traffic Analysis

Ayesha Ajmal
Department of Computer and Information Sciences
Auckland University of Technology
Auckland, New Zealand
ayesha.ajmal@autuni.ac.nz

Maryam Doborjeh
Department of Computer and Information Sciences
Auckland University of Technology
Auckland, New Zealand
maryam.gholami.doborjeh@aut.ac.nz

Jairo Gutierrez
Department of Computer and Information Sciences
Auckland University of Technology
Auckland, New Zealand
jairo.gutierrez@aut.ac.nz

***Abstract*—The rapid growth of fileless malware raises a fundamental challenge to existing cybersecurity frameworks. These malwares operate entirely within a system's volatile memory without creating malicious files on the disk. This research aims to overcome a critical gap in Network Intrusion Detection System (NIDS) by proposing a novel hybrid deep-learning framework. Traditional signature-based detection methods prove ineffective against these memory-resident threats, consequently this investigation details advanced feature extraction methodologies which can identify fileless malware using Network Packet Capture (PCAP) files. This study will employ Design Science Research (DSR) integrating it with a Design-Oriented Machine Learning (DS-ML) methodology which ensures systematic and rigorous development and evaluation process. Key contributions of this research will be: 1) holistic development of feature extraction mechanism that effectively captures fileless malware behavior within network traffic, 2) proposing a hybrid deep-learning model for optimizing the detection techniques for fileless malware, and 3) constituting specific evaluation metrics to measure the accuracy of detecting fileless malware. The resultant framework will discuss the limitations that are present in the existing approaches that primarily focus on detecting file-based malware.**

***Keywords*—Cyber security, Fileless malware, Network traffic, Intrusion detection, Malware traffic, Feature extraction, Memory-resident threats, Design science research**

I. Introduction

The rapid growth of the Internet over the past few decades has revolutionized the societal framework, global economy and basic infrastructure. This era often depicted as the evolution of "cyber civilization". It has changed the perspective of how we seek information and interact with each other. Building on this backdrop, rapid increase in digital adoption and progression in information and communication technology (ICT) have made the information more accessible, but they have also introduced crucial security concerns. The continuous advancements in technology have increased the risk to personal, organizational and societal security. To prevent these threats, various security protocols have emerged which includes the cybersecurity protocols, legal regulations and educational campaigns focused on promoting ethical conduct and risk mitigation [1].

Regardless of the improvements in cybersecurity, many malicious programs continue to evade due to sophisticated obfuscation techniques that enable them to evade traditional, signature-based detection systems. A key constraint of signature-based techniques is the constant need to update signature databases, as cyber-criminals rapidly create variants that contain unique digital fingerprints. For example, the Cisco 2017 Annual Cybersecurity Report revealed that 95% of the malware they analysed was less than 24 hours old, underscoring the swift evolution of malware and the persistent challenges it poses for researchers [2].

Expanding on this point, malwares traditionally stored as an executable file on disk and loaded into memory while execution. In general, this process leaves traces on disk which made it relatively easy for signature-based antivirus (AV) to flag threats through file scanning. However, to evade these security measures, attackers have shifted towards fileless techniques to evade the traditional AV solutions.

Fileless malware differs from traditional threats due to several key characteristics. It operates without a malicious file on the disk which makes it highly complex and difficult to detect. Since it resides in a computer's volatile memory (RAM), a simple system reboot can clear some of its scripts. However, attackers overcome this with sophisticated persistence techniques. They often configure native Windows features like the Task Scheduler, Windows Registry, and Windows Management Instrumentation (WMI) to ensure the malware re-launches after a reboot. The malware also employs various obfuscation methods such as encoding, encryption, string splitting, and data obfuscation to further complicate detection and analysis. This approach makes fileless attacks a challenge for traditional security tools [3].

The remainder of this paper is organized as follows: Section II provides a literature review that examines the background of fileless malware threats and related work in detection methodologies. Section III formulates the research problem and defines the objectives of this study. Section IV outlines the methodology and describes the Design Science Research (DSR) approach integrated with Design-Oriented Machine Learning (DS-ML) and outlines the Machine Learning Process Model (MLPM) phases that will guide the investigation. Finally, Section V concludes the paper with a summary of the research contributions and outlines the next steps in the development and

evaluation of the proposed hybrid deep-learning framework.

II. Literature Review

Fileless malware represents a category of attacks that exploit existing files, legitimate applications and system services to carry out malicious activities without interacting with the file system. These attacks are highly adaptive because they operate by hiding their malicious activities in system's trusted operations.

A. Background

In May 2025, a major cybersecurity breach at Adidas exposed customer data, including names, email addresses, and phone numbers. The company confirmed the incident was a result of a compromise at a third-party service provider, which led to unauthorized access to customer information. Adidas was quick to assure the public that sensitive data, such as payment and password details, remained secure and were not impacted by the breach [4].

Around the same time, the West Lothian Council in Scotland reported a ransomware incident that disrupted operations across various schools and nurseries. The Interlock ransomware group took responsibility for the attack, which resulted in the exposure of various operational records. Authorities also acknowledged the possibility that certain individuals or social work information could have been at risk. The council's immediate response included isolating compromised systems, informing relevant parties, and initiating a formal investigation in cooperation with Scotland Police [5].

Fileless malware is a major concern in today's threat landscape. Unlike traditional threats, these sophisticated attacks leave minimal traces on disk, as they leverage legitimate system tools to achieve their goals. According to the Aqua Security Cloud Native Threat Report (2023) [6], the frequency of fileless attacks have increased approximately 1,400% over the past year. This immense rise highlights a critical shift in the methods used by attackers. Threat actors are exploiting built-in utilities like PowerShell to exfiltrate data from compromised environments, bypassing traditional security systems and detection mechanisms. This makes them particularly difficult to detect and defend against.

B. Related Work

To overcome this limitation, recent research has focused on identifying and mitigating web-based attacks using machine learning algorithms, particularly achieved through extensive feature engineering. The proposed methodology involved fine-tuning the feature extraction process before applying classifiers such as J48 decision tree, Naïve Bayes and OneR. The testing was performed on the publicly available CSIC 2010 HTTP dataset [7].

For detecting malware, researchers presented a comprehensive machine-learning framework by integrating memory forensics with dynamic analysis. The process began by generating a specialised dataset using Cuckoo Sandbox to analyse malware and volatility to capture memory dumps. Feature extraction was performed on these memory dumps which includes process behavior, dynamic link libraries, network events and registry modifications. These features are then evaluated on multiple machine-learning classifiers such as Random Forest, Decision Tree, Gradient Boosting and K-Nearest Neighbours to identify the most effective model. The findings revealed that the Random Forest classifier achieved the highest accuracy, underscoring the potential of combining dynamic memory analysis with a robust machine learning approach for effective malware detection [8].

Fileless malware is host-independent malware, it does not require any host file to execute. These attacks can easily avoid traditional detection system. To detect and analyze fileless malware, memory-based (volatile memory forensics) technique was used [9]. The study utilized a comprehensive dataset of 1249 Windows-based fileless malware samples along with which Kovter malware was included to validate the approach. The data in the volatile memory used as a memory dump along with registry and network monitoring. To further examine the data, Process Explorer, Autoruns and Wireshark were used. The results depict that the combination of memory forensics with behavioral and registry analytics gives more accurate identification and characterization of fileless malware. However, integrating machine learning methodologies can help automate detection and strengthen the emerging attack strategies.

To explore the strategies of detecting fileless malware on Windows systems, researchers focus on sophisticated attacks by fileless malware that operate entirely in memory and leave minimal traces behind. The researchers cyberattack tactics and techniques to enhance malware detection. Hera collects and correlates artifacts from multiple sources like running processes, registry entries, event logs, WMI, networks, and files to spot suspicious behaviors associated with these attacks, such as persistence and stealthy discovery techniques. The study uses a dataset of well-known fileless malware samples, including Kovter, Trickbot, and AgentTesla, collected from public malware repositories. When put to the test, Hera shows clear results over popular alternatives like Loki and Thor Lite, detecting a wider range of malicious activities and completing scans much faster. Overall, the paper demonstrates how Hera effectively leverages ATT&CK knowledge for practical, efficient detection, providing security professionals with detailed insights and actionable reports for defending against fileless cyber threats [10].

Building on this, the authors of another study [11] designed a malware detection framework that also used memory forensics but with a different approach. They executed various malicious software samples, including rootkits, Trojans, and ransomware, in a virtual environment to obtain memory dumps. Using the Volatility tool, they extracted a comprehensive set of features, such as process details, loaded modules, and network connections. The dataset for this study was comprised of memory dumps from controlled experiments featuring various malware families and benign programs on a Windows platform. It included real-world samples of advanced threats that use memory-only and obfuscated execution techniques. The dataset

was designed to represent diverse malware behaviors, enabling models to learn subtle differences based on in-memory artifacts.

According to the report published in Global Overview, population data from the United Nations signifies that there are 8.20 billion humans living on Earth today. A total of 5.56 billion people uses the Internet at the start of 2025 [12]. The Internet has been extremely susceptible to malicious attacks and activities which in return affect its performance. Network intrusions critically disrupt Internet connectivity which leads to substantial financial losses.

Network Intrusion Detection Systems (NIDS) is one of the important tools that are used to observe and identify malicious activities in network traffic. However, traditional NIDS are now facing challenges due to the rapid increase of data volumes and complex attacking strategies. Lately, artificial intelligence is making advancements, specifically in the field of deep learning. Recent contributions in NIDS have improved detection accuracy and validation by using deep-learning, specifically the 1D-CNN model. It was evaluated using the NF-UQ-NIDS-v2 dataset which comprised several smaller datasets that provide a comprehensive representation of real-world traffic. The model effectively detected benign traffic, Distributed Denial of Service (DDoS), Denial of service (DOS), scanning and bot attacks. Their deep learning 1D-CNN model with regularization yields excellent results with an accuracy of 94.0% [13].

III. Research Problem and Objectives

A. Research Problem

Despite the steady progress in the development of detection techniques, a clear research gap persists in the context of fileless malware. While recent studies cover a broad spectrum from feature extraction and integration of memory forensics with dynamic analysis to advance deep-learning models, most studies either focus on file-based threats or fail to validate their methods against genuine fileless malware that can infect our system through network traffic.

B. Objectives

The main objective of this research is to develop a novel approach based on machine-learning detection framework to identify fileless malware threats that transmits through network-traffic. This study aims to address the fundamental cyber-security gap in identifying advanced evasion techniques that are exploited by malicious attackers. These attackers utilize legitimate system tools such as PowerShell and Windows Management Instrumentation (WMI) to execute malicious activities, that leaves no traces on the disk. By implementing deep learning methods and performing advance feature extraction methodologies within a Network Intrusion Detection System (NIDS), this research intends to overcome the limitations of signature-based detection systems that fail against the rising threat of fileless malware attacks. However, this research will answer the following questions:

RQ1: How do theoretical frameworks of hybrid deep learning contribute to advancements in fileless malware detection, and what are the limitations of these frameworks in addressing emerging fileless malware threats?

RQ2: What innovative approaches within hybrid deep learning could be formulated as a framework to address the challenges of real-time detection and prevention of fileless malware in dynamic and complex network environments?

*a)*How does the inclusion of critical temporal and sequential attributes from PCAP files impact the accuracy and reliability of the proposed framework?

*b)*What is the relationship between the preservation of behavioral indicators in network captures and the interpretability of the models included in the framework?

RQ3: How can we critically evaluate the proposed framework compared to existing deep-learning models?

IV. Methodology

This study is based on the Design Science Research (DSR) paradigm, which emphasizes generating an innovative solution to address a real-world problem. Given the data-driven and practical nature of this study, we applied a specialized subclass of DSR known as Design-Oriented Machine Learning (DS-ML). This approach is crucial for developing novel solutions for complex problems, such as fileless malware detection, which are not properly addressed by traditional methods.

This research will follow the Machine Learning Process Model (MLPM) as proposed in [14], to ensure a structured, systematic and academically comprehensive approach. This hybrid framework integrates with the practical and iterative cycles of Cross-Industry Standard Process for Data Mining (CRISP-DM) with the academic rigorous standards of DSR, which also includes reflective elements of Action Design Research (ADR). Fig. 1, illustrates the proposed process model (MLPM) for ML studies. This research process is focused on the following key phases of the MLPM:

*a) Problem Identification and Motivation:*This is a fundamental phase in which we identify the critical and increasing problems of fileless malware. Unlike traditional malware, fileless malwares operate solely in memory and do not write any malicious code on disk which makes them hard to detect using conventional signature-based detection systems. It creates a significant threat to organizations and compromises the integrity and security of personal data. This highlights the critical need for a more robust and effective detection mechanism.

*b) Objective Formulation:*The primary objective of this study involves design, develop and evaluate a hybrid deep learning framework which is capable of effectively detecting fileless malware from network traffic. The architecture of this framework will integrate both static and dynamic features to improve the detection accuracy and enhanced resilience against advanced evasive techniques. Secondary objective comprises of the generalization of findings into scalable design principles that can be broadly applied to resolve broader challenges across the cybersecurity domain.

*c) Data Analysis and Preparation:*These two phases are interconnected with our data-centric approach. For this research,

comprehensive datasets, that are publicly available, will be acquired that contains both benign and fileless malware samples. In the data interpretation phase, data exploration and visualization will be performed to identify the patterns and in-consistencies, which will then proceed to data preparation. In this crucial time-intensive phase, cleaning of raw data, handling missing values, feature normalization and feature selection will be carried out to enhance the performance of the model. We will be following an iterative approach, that will allow us to revisit this phase if issues are identified during the later stages of the research.

*d) Design, Development and Refinement (DDR):*This phase is a core of this research, where theoretical objectives are interpreted into tangible artifacts. We will create and develop the hybrid deep learning framework which will facilitate our research contributions. This phase will enable us to explore our innovative architectural concepts and reasoning to justify our development decisions based on relevant theoretical knowledge. The DDR phase is highly iterative, involve cycles of model training, testing and validation. We will use techniques such as cross-validation and hyperparameter tuning to optimize the key performance metrics such as f1-score, accuracy, precision and recall.

*e) Evaluation:*The effectiveness of our artifacts will be precisely evaluated against the objectives established in Phase 2. We will use a dedicated test dataset to validate the performance of the model. The evaluation will assess its ability to accurately detect and classify fileless malware samples while minimizing false positives, thereby demonstrating its functionality and performance compared to existing solutions.

*f) Reflection and Learning:*This phase is critical for the scientific contributions of this research. We will transcend the specific artifacts to generalize our findings. This includes analysis of model's features and behavior to derive generalised principles and a set of guidelines for building effective fileless malware detection systems.

*g) Communication:*The final phase involves communicating the findings of the research to both the scholarly and professional publications. We will document our methodology, developed artifacts and results in a scholarly publication to disseminate our work and contribute to the body of knowledge in cybersecurity.

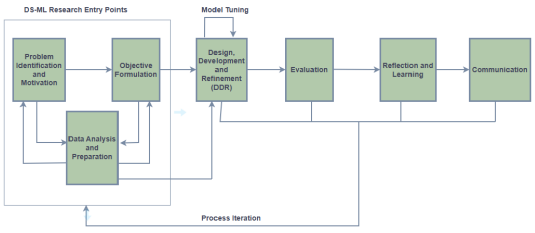

Fig. 1. MLPM Process Model

V. Conclusions

The key purpose of this research is to develop a novel deep-learning framework to identify fileless malware attacks that are transmitted through network traffic which addresses a key cyber-security research gap in detecting advanced evasion techniques. The next step involves the Design, Development and Refinement (DDR) phase, which is the core of this research. During this phase, a hybrid deep-learning framework will be developed which will then be refined through iterative cycles of model training, testing and validation. The effectiveness of the model will then be evaluated by using a dedicated testing dataset. This evaluation will assess the ability of the model to accurately detect fileless malware samples with minimum false positives.

References

[1] W. S. Admass, Y. Y. Munaye, and A. A. Diro, "Cyber security: State of the art, challenges and future directions," *Cyber Secur. Appl.*, vol. 2, p. 100031, 2024, doi: 10.1016/j.csa.2023.100031.

[2] O. P. Samantray, S. N. Tripathy, and S. K. Das, "Notice of Violation of IEEE Publication Principles: A study to Understand Malware Behavior through Malware Analysis," in *2019 IEEE International Conference on System, Computation, Automation and Networking (ICSCAN)*, Pondicherry, India: IEEE, Mar. 2019, pp. 1–5. doi: 10.1109/ICSCAN.2019.8878680.

[3] S. Liu, G. Peng, H. Zeng, and J. Fu, "A survey on the evolution of fileless attacks and detection techniques," *Comput. Secur.*, vol. 137, p. 103653, Feb. 2024, doi: 10.1016/j.cose.2023.103653.

[4] "Adidas says customer data stolen in cyber attack." Accessed: July 09, 2025. [Online]. Available: https://www.bbc.com/news/articles/c071m82v80po

[5] "Sensitive data stolen in West Lothian cyber attack." Accessed: July 09, 2025. [Online]. Available: https://www.bbc.com/news/articles/cpw77gj8v98o

[6] "Fileless Malware - The Invisible Threat You Need to Know About." Accessed: July 09, 2025. [Online]. Available: https://amatas.com/blog/fileless-malware-the-stealthy-threat-you-need-to-know-about/

[7] S. Sharma, P. Zavarsky, and S. Butakov, "Machine Learning based Intrusion Detection System for Web-Based Attacks," in *2020 IEEE 6th Intl Conference on Big Data Security on Cloud (BigDataSecurity), IEEE Intl Conference on High Performance and Smart Computing, (HPSC) and IEEE Intl Conference on Intelligent Data and Security (IDS)*, Baltimore, MD, USA: IEEE, May 2020, pp. 227–230. doi: 10.1109/BigDataSecurity-HPSC-IDS49724.2020.00048.

[8] I. J. Ezeonwu and S. M. Musa, "Comparative Analysis of Machine Learning Classifiers for Fileless Malware Detection," in *2024 International Conference on Green Energy, Computing and Sustainable Technology (GECOST)*, Miri Sarawak, Malaysia: IEEE, Jan. 2024, pp. 1–6. doi: 10.1109/gecost60902.2024.10474708.

[9] I. Kara, "Fileless malware threats: Recent advances, analysis approach through memory forensics and research challenges," *Expert Syst. Appl.*, vol. 214, p. 119133, Mar. 2023, doi: 10.1016/j.eswa.2022.119133.

[10] T.-G. Nguyen et al., "Detecting Fileless Malware on Windows with ATT&CK: A Practical Approach," in *2024 International Conference on Electrical, Computer and Energy Technologies (ICECET)*, Sydney, Australia: IEEE, July 2024, pp. 1–6. doi: 10.1109/icecet61485.2024.10698218.

[11] S. Zhang, C. Hu, L. Wang, M. Mihaljevic, S. Xu, and T. Lan, "A Malware Detection Approach Based on Deep Learning and Memory Forensics," *Symmetry*, vol. 15, no. 3, p. 758, Mar. 2023, doi: 10.3390/sym15030758.

[12] "Digital 2025: Global Overview Report," *DataReportal – Global Digital Insights*. Accessed: Sept. 10, 2025. [Online]. Available: https://datareportal.com/reports/digital-2025-global-overview-report

[13] A. Setiawan, A. M. Widodo, G. Firmansyah, N. S. Fatonah, B. Tjahjono, and A. Wisnujati, "Network Intrusion Detection Using 1D Convolutional Neural Networks," in *2024 4th International Conference on Electronic and Electrical Engineering and Intelligent System (ICE3IS)*, Yogyakarta, Indonesia: IEEE, Aug. 2024, pp. 415–419. doi: 10.1109/ICE3IS62977.2024.10775512.

[14] H. Zolbanin and B. Aubert, "A process model for design-oriented machine learning research in information systems," *J. Strateg. Inf. Syst.*, vol. 34, no. 1, p. 101868, Mar. 2025, doi: 10.1016/j.jsis.2024.101868.