THE ASIAN BULLETIN OF BIG DATA MANAGEMENT
Vol.4. Issue4 (2024)
https://doi.org/ 10.62019/abbdm.v5i1.289

ML-based Fileless Malware Threats Analysis for the Detection of Cyber security Attack based on Memory Forensics: A Survey

Ahmad Mujtaba*, Mehrunisa Zulfiqar, Muhammad Umar Azhar, Sadaqat Ali, Asfar Ali, Hamayun Khan

Chronicle

Article history

Received: Oct 12, 2024
Received in the **revised format:** Oct 29, 2024
Accepted: January 11, 2025
Available online: January 27, 2025

Ahmad Mujtaba*, Mehrunisa Zulfiqar, Sadaqat Ali, Asfar Ali, and Hamayun Khan are currently affiliated with Faculty of Computer Science & IT Superior University Lahore, Pakistan.
Email: hafizxholics178@gmail.com
Email: Mehrunisa840@gmail.com.
Email: sa.sadaqat.ali20@gmail.com
Email: asfarali761@gmail.com
Email: hamayun.khan@superior.edu.pk

Muhammad Umar Azhar currently affiliated with Department of Computer Science, National University of Computer and Emerging Sciences (FAST-NUCES), Lahore, 54000, Pakistan and also affiliated with Share Mobility
Email: umarazhar235@gmail.com

Corresponding Author*

Abstract

The rapid advancements in cyber-attack strategies are in parallel with the measures for detection, analysis, and prevention. Attackers have recently developed fileless malware that can simply bypass existing security mechanisms. The high complexity of malware and the attacks rises in today's world because malware increases the chance of cyberwar in many countries, the rise of one of the most sophisticated fileless malware is now increasing day by day and the present challenges for traditional malware detection and analysis are used that does not provide the complete information on Fileless malware. It evades conventional signature and firewall detection systems by hiding and directly injecting its malicious code into RAM, leaving no or minimum traces on the file system. This review paper explores the crucial artifacts in memory forensics that lead to a critical approach to addressing the challenges mentioned so that the investigator can detect and analyze the critical threats. Also, it highlights the method that helps the investigators analyze every aspect of the malicious or embedded code. This will help us to improve the detection criteria and the accuracy of the results. This study also helps the examiners in the examination of the processes and different types of analysis i.e. strings, anomaly detection, and the critical techniques used for retrieving malware artifacts. This review also includes the limitations of the existing tools and methodologies and the new evolving techniques and tactics used by the malware to hide its footprints. By identifying these gaps these papers provide robust farmwork for the enhancement of malware analysis tools and procedures to help the examiners in the analysis and examination of malware.

Keywords: Memory artifacts, Fileless Malware, Malware investigation, Cybersecurity, Executable Files Analysis, Anti-Forensics, Incident Response, Signature-Based Detection, Fileless Malware Detection.

INTRODUCTION

The rapid growth in cyber security and internet security has been witnessed in the rapid development of many new types of cyber-attacks and in today's world these attacks have become more sophisticated. One of the attacks that was used by many threat actors is malware attacks that once deployed in the user system remove their tracks and perform harmful activities [1]. According to Av-test institutes, more than 45.000 new malware and unwanted apps are registered daily and they impose a greater threat on today's system. The old antivirus solution relies on static and heuristic techniques for the detection of these malware, but modern malware uses advanced encryption and cryptographic techniques so that these antiviruses can't identify them [2, 3].

There are different types of malware but among them, one of them is fileless malware which gains significant importance due to its nature of evading detection from antiviruses. Unlike other malware that leaves a track on the operating system, this

malware leaves no track on disk-resident files and leaves minimal or no artifact behind exploiting the CVes and system tools in legitimate software [4, 5]. This unique way provides a way to bypass the system antivirus software and signature-based detection techniques and maintain its persistence in the system. Making it harder for detection [6].

To overcome these threats in today's world cybersecurity researchers have also provided a way to investigate these types of threats using modern forensics techniques like memory forensics a domain in forensics that helps in the analysis of the memory to see the malicious processes and helps to analyze the internal state of the operating system like the running processes, user processes, kernel processes [7, 8]. In the traditional analysis, the examiner can't see the complete picture of malware as these malware have modern cryptographic techniques which help them to leave no or minimal traces but the modern forensic techniques like memory analysis provide a Unique way like process analysis, entropy and strings imported and the PE analysis which pays a great role in the identification of these threats [9].

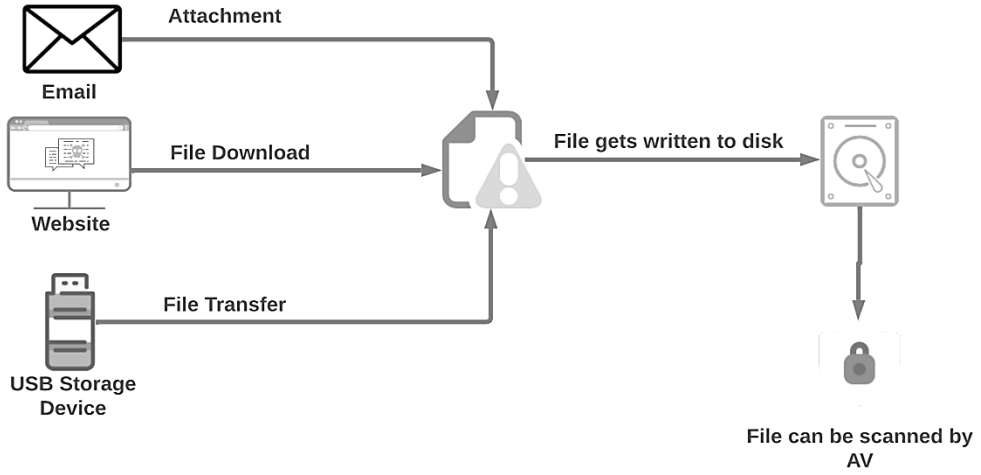

Figure 1: Malware chain based on File [10]

This paper comes up with the field of malware analysis and memory forensics in many ways:

- Describing Fileless Malware: This paper delves into the detection of malware that is fileless in nature and the artifacts obtained from the analysis of the memory.
- Forensic investigation Techniques: The importance of the advanced forensic investigation tools and how to use those tools to analyze the processes and DLL which helps to understand the persistent behavior of malware in the memory [11].

The advancement of today's malware has made a great impact on today's world as its detection mechanism and its analysis prove difficult with traditional forensic techniques. The signature-based detection has proved efficient against traditional malware but like fileless malware which can't detect easily these traditional techniques can't apply to them also with the greater development of polymorphic malware which modifies its code and can't detect heuristic-based detection techniques. The examiners face limitations in their analysis when addressing these types of evasion techniques such as cryptographic encryption and code obfuscation [12, 13]. Malware is a program that is used by attackers to gain unauthorized access to some network or system which will lead them to obtain their data. In general, it is a

piece of malicious code that executes itself once it enters the victim system and then it starts spreading depending on the nature of what it was designed for it will spread over the network and exploit any available services or device tool, etc. its main objective is to disrupt the system and cause damage as much as possible [14, 15]. Most of the attackers send it using emails, word documents, USB sticks, or as attachable downloads or in the form of free software. Malware is divided into various types depending on the code and specifically the information needed.

Table 1.

Comparative Analysis of state of-the-art Approaches

	Type of Malware	Vulnerabilities Exploitation	Analysis Technique	Dataset Used	Classification
[10]	In memory attack	Javascript and HTML5	Tested on anti-malware detection tools	NA	No
[8]	In memory and registry attacks, non portable executable	Macros, scripts, registry values, Powershell, SMB payload, obfuscated code, DLL files etc.	Analyzed published and Kuckoo Sandbox samples attack mapped with MITRE	Collected samples from hybrid analysis and GitHub	Yes
[21]	In-memory attack	Shell commands, file system, data-flow, SSH server in IoT	By Profiling four s/w and h/w honeypots in multiple public cloud	NA	No
[24]	In-browser cryptojacking attacks	PowerShell, WMI, scheduler, and registry	Patterns of Fileless malware for Tactics, Techniques, and Procedures	NA	Yes
[9]	In memory and browser-based attacks	Shell commands, file system, SMB, macro, browsers	NA	NA	Yes
[11]	In system and in network attacks	Windows Registry Task scheduler WMI etc.,	Runtime behavior of the system	NA	No
[16]	In sensors memory	IoT devices and edge computing devices	ML-based model with sigmoid function	NA	Yes
[28]	In-Memory attacks	Windows PowerShell scripts	Analysis of registry, commands and windows security logs, abnormal processes	Own Dataset (RAM dump)	Yes

Fileless malware is one of the deadly malware that once deployed in the system removes its traces to a minimum and operates entirely in the memory of the operating system. This malware leaves no traces on the hard disk making it difficult for the examiners to investigate it also it can't be detected using the old traditional forensic methods [16, 17]. Now in today's world, the internet is freely available everywhere and sensitive information is traveling using the internet and as we know it.

Table 2.
Feature Selection Approaches [18]

Feature selection technique	Description
Mutual Information (MI)	Mutual information quantifies the relationship between individual features and the target variable by measuring the information a feature provides about the target variable, independent of other features.
Term Frequency-Inverse document frequency (TF-IDF)	TF-IDF is a widely used method for identifying significant words in a document by measuring their frequency in a collection of documents known as a corpus. This technique is beneficial in automated malware analysis as it maintains human-readable aspects, allowing experts to interpret the data effectively TF–IDF–IDF is calculated by multiplying a word's term frequency and inverse document frequency. A high TF-IDF score indicates that a word is frequent in the current document and rare in other documents, making it a robust discriminator of the document's content.
Principal Component Analysis (PCA)	PCA is a crucial technique for reducing the dimensionality of many correlated features. It aims to identify the directions that capture the maximum variance in the given data.
Information Gain (IG)	This method identifies the optimal features by assigning weights to the information and emphasizing its relevance.
Correlation-based Feature Selection (CFS)	Correlation-based Feature Selection (CFS) is a filter method for feature selection that aims to identify highly correlated features with the target variable while minimizing redundancy among selected features.
Maximum relevance and minimum Redundancy (mRmR)	The mRmR algorithm is a widely recognized filter method designed to identify features with a high correlation (relevance) to the target class and a low correlation (redundancy) to other features.

LITERATURE REVIEW

The cybercriminals' primary goal is to steal this sensitive information, including our account info and personal info and to disrupt the services available to us also some attackers do it for financial gain. The other goal of cyber criminals is to obtain the data as much as possible and for this purpose specifically, they design a malware known as a keylogger that steals the information from the user and sells it on dark forums. E.g. many keyloggers were deployed in the bank to steal credit card information [25, 26]. Malware is also deployed in cyber espionage and for surveillance in cyberspace. The

main goal of this is to listen to the communication between two people to steal business info or gather information related to targets. For this purpose, they design trojan horses that spread in the network and attackers gain access to the network. Most of the time the malware is used for the targeted attack. These are the attacks that are specifically designed for an individual user or corporate or a country [27, 28]. They are designed in such a way so that they can't easily be detected and maintain their persistence for a long time.

Memory forensics is a type of digital forensics that helps the examiners to investigate the activity related to memory. Memory forensics is a crucial part of cybersecurity as with the help of this we can identify the maximum behavior of the malware and investigate the memory processes and DLLs. Memory Forensics contains different types of tools that help in the investigation, collection, and analysis of memory artifacts [29]. This malware was used by many attackers to show no footprints of their action and using this malware that operates entirely within the system memory leaves no traces on the disk that will be difficult for the examiners. Memory forensics plays a crucial role when identifying these types of malware as they only operate in the memory and evade traditional forensic detection tools and antivirus programs [30].

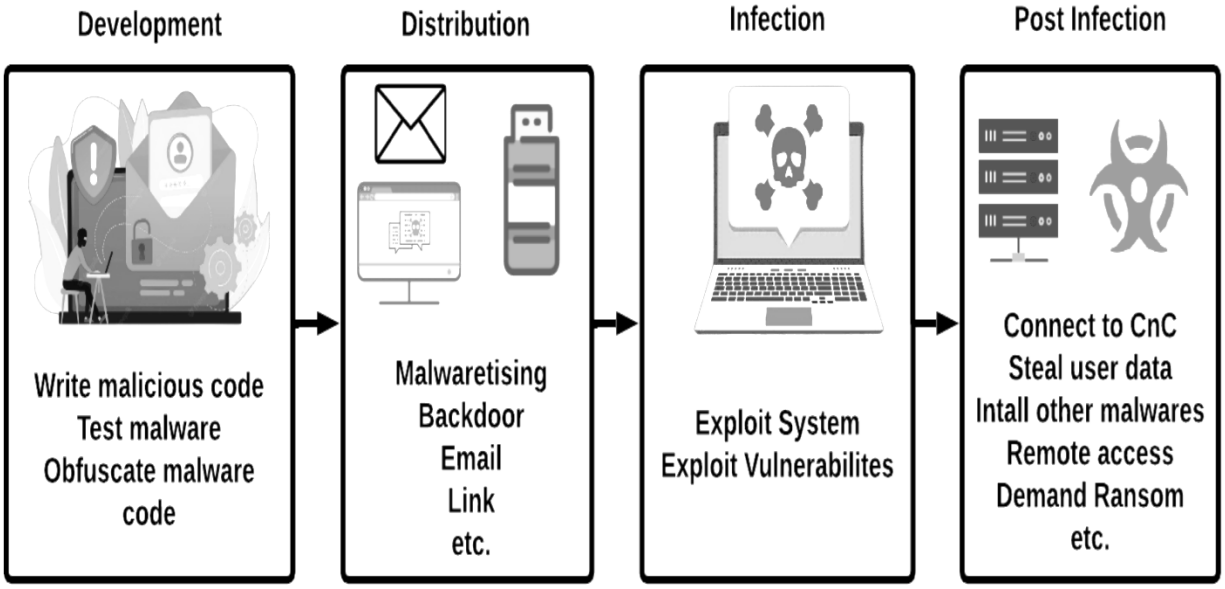

Figure 2.
Life cycle of Malware [31]

By examining the memory for suspicious processes and DLLs used also the APIs used for call making the examiner can find important artifacts related to any malware. The main techniques used for the analysis of memory are memory injections and uncovering the persistence mechanism of any malware [32, 33].

Table 3.
Static Features of File [34]

Types of static features	Examples	Description
File Hashes	MD5, SHA-1, SHA-256	Hashing samples can detect ransomware by matching against a database of known hashes, but attackers can evade these defences by modifying the ransomware slightly.
Header Information	PE header, file format	The file structure and format of the malware executable can reveal its malicious characteristics. Researchers analyze headers, sections, and symbols to determine information in the executable
Function/API Calls/System calls	Imported functions/API	Ransomware uses APIs for encryption, memory management, and network operations. The strings generated from samples can reveal signs of ransomware activity.
Strings	Embedded text strings	Ransomware strings include URLs, messages, bitcoin details, and encoded data, serving as indicators of attacks.
Opcodes	Assembly-level instructions	Analyzing instruction opcodes and patterns in executable code effectively identifies ransomware samples.
File Types	File extensions and formats	It means the type of files that are targeted by ransomware for encryption.

Memory Injections in Legitimate Processes

Most of the attacker's favorite tactics used during fileless malware execution is memory injection which is the insertion of a malicious code into one of the trusted processes of the memory. This way malware can hide its presence from the traditional analysis. As the malicious code is directly injected into the legitimate process it is difficult to identify the malware using the traditional forensic approach. Memory forensics can identify these types of malware using the active memory processes by analyzing the different portions of the memory allocated to the processes or by analyzing the API calls, malicious code, or unusual system calls. By analyzing these portions, security researchers can identify the malware artifacts present in the memory and thus neutralize the threat [35, 36].

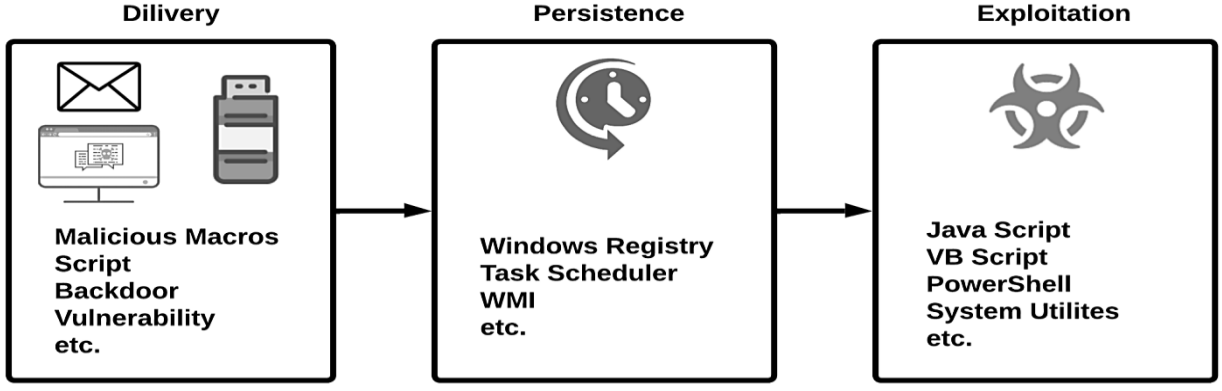

Figure 3.

Life cycle of Malware (Fileless) [37]

Persistence Mechanisms: Registry-based Execution and DLL Sideloading

The registry is the part of the Operating system that tracks every activity of software the fileless malware was used in the registry to change the exe values so that persistence can be maintained. While the other method includes DLL sideloading. Registry-based execution allows the malware to store and execute malicious code from the system registry, which is often overlooked by traditional detection tools [38, 39]. Memory forensics can help identify such threats by analyzing the system's memory for registry entries that are abnormal or linked to suspicious activities [40, 41]. DLL sideloading is another technique used by fileless malware, where the malware loads a malicious Dynamic Link Library (DLL) file into a legitimate application. This allows the malware to run under the guise of a trusted application, making detection more challenging. By analyzing memory artifacts, such as loaded DLLs and their associated processes, memory forensics can identify the presence of malicious DLLs and the process they are running within. This information helps security professionals track and mitigate the malware's persistence mechanisms [42, 43].

MATERIALS AND METHOD

Segmentation is the breaking of large memory dumps into smaller regions so that analysis can be conducted easily. The detection of memory modification and memory injection and the behavior of malicious code were reviewed. Malicious apps are analyzed using their API calls and their memory addresses and the behavior of the PE and they were compared to analyzing suspicious behavior. The volatile memory technique was also used for the analysis of fileless malware behavior to identify its TTPs.

Dynamic Link Library (DLL)
Several memory techniques were used to identify the DLLs that were loaded into the memory and analyzed them to view the anomalies and libraries they are linked to and the unsigned libraries that help the malware evade detection [44, 45].

Event Log Correlation
The event log was analyzed with memory to see the correlation between memory artifact and the event log also it helped us to analyze the unauthorized malicious activities such as unregistered software and commands. Studies using signature-based approaches for detecting known patterns in memory, such as PE headers or obfuscated code, were examined. Approaches utilizing entropy analysis to identify regions with high randomness indicative of packed or encrypted malware were reviewed. Techniques for detecting API hooking attempts by malware to hijack legitimate system functions were evaluated [46, 47].

Fileless Malware Detection
Emphasis was placed on methods specifically targeting fileless malware, such as detecting malicious scripts and memory-resident code that do not leave disk artifacts. The memory results were crossly referenced with the signed processes to reduce the chances of false positives and improve the accuracy of the results. The analysis of memory forensic methodologies for the detection of fileless malware provided us with valuable insight into the analysis of fileless malware tools, techniques, tactics,

procedures, strengths, weaknesses, and limitations. The results are categorized depending on the focus areas of this paper including the collection, analysis, and detection strategies of fileless malware in memory forensics [48].

Static Sample Collection

Samples from malshare and malware db. Provide a great insight into the comparison of PE files for the baseline comparison. The legal software from their official websites such as Kaspersky and Microsoft was effective in the behavior analysis of the standard libraries, Processes, and DLLs [49]. These samples were only valuable in the identification of signature-based malicious threats but inadequate for the detection of runtime malicious behavior.

Dynamic Sample Collection

The dumps gathered from the memory using the sandbox provide more information about the malicious exe runtime behavior as compared to the static collection. Analysis of memory dumps exposed injected code, anomalous DLL loading, and memory-resident malware that evades traditional disk-based detection. Fileless malware often executes and disappears quickly, making timely data collection critical. Techniques for reliably capturing volatile memory data during execution remain inconsistent across studies [50].

Table 4: Fileless malware samples [51]

SR.	Name of Website	Description	Owned By	No. of Malware Samples Available	No. of Fileless Malware Samples Available and Downloaded
1	VirusShare	A repository of live malware samples with malicious code	Corvus Forensics	55,372,441	11
2	AnyRun	An online interactive sandbox with a vast malware sample database	AnyRun	6,200,000	10
3	PolySwarm	A crowdsourced threat detection marketplace	PolySwarm	350,000	5

MEMORY ANALYSIS

Process and DLL Inspection

Techniques for extracting and analyzing processes and DLLs from memory dumps were widely discussed. Studies identified unsigned DLLs and unusual API calls as common indicators of malicious activity. Memory segmentation was effective in isolating malicious regions for detailed analysis [52]. Anomalies such as excessive memory usage, unauthorized process spawning, and unusual inter-process communications were consistently flagged as suspicious. Behavioral analysis was especially effective in detecting stealthy fileless malware that avoids traditional

signature-based detection. Process-based analysis often struggles with heavily obfuscated or encrypted code. Detection accuracy was highly dependent on the quality of the baseline process behavior data.

Detection Strategies

Signature-based approaches were effective against known threats but inadequate for identifying zero-day or obfuscated fileless malware.

Entropy Analysis

High entropy regions within memory dumps reliably indicated the presence of packed or encrypted malicious code. However, entropy analysis alone was insufficient for providing actionable intelligence without additional context.

API Hook Detection

Detecting API hooks proved to be a robust method for identifying fileless malware manipulating system functions. This approach was particularly effective in uncovering stealthy lateral movement techniques used by attackers.

Event Log Correlation

Combining memory data with event log analysis enhanced detection accuracy by providing a holistic view of system activity. However, the method used for this purpose requires a comprehensive number of resources and expertise to execute effectively Malware that doesn't show traces on disk and resides in the memory like fileless malware can be very difficult to analyze using old tools and that is why memory forensics gives us great artifacts in file malware cases. The techniques of using behavior analysis, Process analysis, and Dll analysis play an effective role than traditional tools, especially for fileless malware that has no footprints on disk [53]. The persistence mechanism of this malware like making WMI calls and the abuse of PowerShell commands and tools like space were found to an important attack vector

Research Gaps & Challenges in Memory Forensics

The need for forensics in memory was important as malware is changing their way of action day by day but it comes with several challenges that minimize the efficiency of this process. These challenges include Evasion Techniques, The tool's limitations, and scalability, which complicate the memory forensic analysis process. Additionally, some ethical and regulatory challenges come into play when we are talking about memory forensics. But now the courts are accepting the memory forensic as legal evidence in court hearings, and it was easily admissible in the court.

Evasion Techniques

As the threat becomes more advanced and changes their attack of chain continuously it is difficult for the cyber security professionals to identify them with old methods. Nowadays malware uses such a mechanism that they obfuscate their code and use encryption so that it is not in readable form and no one can read it and the result is it will automatically show no traces on the disk and run as a legitimate process in the memory. When a code is obfuscated, the attacker hides the code in the streams and makes it difficult for the forensic tools to extract and analyze it. While in encryption they encrypt their code which will change its signature and thus remain undetected from the detection tools. To minimize these types of false analyses memory forensics must be advanced in the evasion detection techniques. The major challenge in this era is the tool as the cyber threats keep advancing there is a lack of advanced tools to analyze cyber-attacks. This lack of standardization in the memory forensic tools becomes a major problem when analyzing memory dumps. Each tool produced has some missing functionality and data formats which results in inconsistent analyses of the forensic artifacts. During the analysis, we can't rely on a single result we have to perform it multiple times to remove the chances of error and produce correct results which is a time-consuming method also sometimes we have

to deal with encryption which also takes time to break and every tool does not contain all these properties. So, there is a need for tool standardization among these tools to ensure a smooth memory analysis process across different Platforms.

Ethical and Regulatory Challenges

Sometimes memory forensics contains personal data like passwords, private internet communications and browsing data which is a user's private information and its misuse is unethical. So, to respect everyone's privacy rights we have to be ethical and follow the proper procedure while accessing this type of data during analysis. Sometimes some regulatory frameworks have to be followed for the analysis part to avoid the misuse of private information in cyber security. Which varies on the jurisdiction and context of every society.

CONCLUSION

The severe issue of the fileless malware cyber threat could block or restrict people from accessing their systems or data. Fileless malware represents a significant challenge to traditional cybersecurity defenses, as it operates entirely in memory and utilizes legitimate system tools, making it difficult to detect and mitigate using conventional methods This paper highlights the role of memory forensics specific to the challenges posed by the fileless malware in today's world, which helps us to understand how they remain silent to avoid detection from traditional tools like disk-based detection methods. The indicators found in the memory like unsigned processes and the DLL injection, Process injection, and other artifacts provide a great way to identify these types of malware. The thorough analysis reveals that by doing the static analysis of memory these malware can't be identified because they are inaccessible through static technique or signature-based detection. The study also reveals that the analysis of several memory portions and processes using memory forensics provides a critical role in the detection and analysis of these types of malware. Some gaps need to be filled to analyze the malware, including the lack of standardized data sets, detection in real-time, and the number of resources and techniques used for the analysis part. This paper concludes that memory forensics plays a vital role in the detection of fileless malware by analyzing the volatile memory and presenting unique artifacts of malicious activities. For further process enhancements and accuracy for future research the development of real-time detection capabilities, the creation of improved memory datasets, and optimized resources are needed. In conclusion, the dynamic and volatile nature of memory makes it an invaluable resource for malware detection, offering unique insights into the activities of malicious software. To enhance its efficacy, future research should focus on developing real-time detection capabilities, creating comprehensive memory datasets for benchmarking, and optimizing resource utilization. These advancements will not only improve the detection and response to fileless malware but also strengthen overall cybersecurity frameworks in the face of evolving threats.

REFERENCES

1. Tahir, R. A study on malware and malware detection techniques. Int. J. Educ. Manag. Eng. 2018, 8, 20. [Google Scholar] [CrossRef] [Green Version]
2. Leukfeldt, E.R.; Kleemans, E.R.; Stol, W.P. Cybercriminal networks, social ties and online forums: Social ties versus digital ties within phishing and malware networks. Br. J.

Criminol. 2017, 57, 704–722. [Google Scholar] [CrossRef]
3. Alenezi, M.N.; Alabdulrazzaq, H.; Alshaher, A.A.; Alkharang, M.M. Evolution of malware threats and techniques: A review. Int. J. Commun. Netw. Inf. Secur. 2020, 12, 326–337. [Google Scholar]
4. Smelcer, J. Rise of Fileless Malware. Ph.D. Thesis, Utica College, Utica, NY, USA, 2017. [Google Scholar]
5. New Ponemon Institute Study: Key Findings the 2017 State of Endpoint. Available online: https://www.ponemon.org/news-updates/blog/security/the-2017-state-of-endpoint-security-risk-report.html (accessed on 11 November 2021).
6. https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0043-x An Emerging Threat: Fileless Malware - A Survey and Research Directions.
7. Ghafir, I., Hammoudeh, M., Prenosil, V., Han, L., Hegarty, R., Rabie, K., & Aparicio-Navarro, F. J. (2018). Detection of advanced persistent threat using machine-learning correlation analysis. Future Generation Computer Systems, 89, 349-359.
8. Joloudari, J. H., Haderbadi, M., Mashmool, A., GhasemiGol, M., Band, S. S., & Mosavi, A. (2020). Early detection of the advanced persistent threat attack using performance analysis of deep learning. IEEE Access, 8, 186125-186137.
9. Reddy, B. I., & Srikanth, V. (2019). Review on wireless security protocols (WEP, WPA, WPA2 & WPA3). International Journal of Scientific Research in Computer Science, Engineering and Information Technology, 5(4), 28-35.
10. Halbouni, A., Ong, L. Y., & Leow, M. C. (2023). Wireless Security Protocols WPA3: A Systematic Literature Review. IEEE Access.
11. Ambavkar, P. S., Patil, P. U., Meshram, B. B., & Swamy, P. K. (2012). Wpa exploitation in the world of wireless network. Int J Adv Res Comput Eng Technol, 1(4), 609-618.
12. Cahyadi, D., Astuti, I. F., & Nazaruddin, N. (2023, February). Comparison of throughput and CPU usage between WPA3 and WPA2 security methods on wireless networks 802.11 n. In AIP Conference Proceedings (Vol. 2482, No. 1). AIP Publishing.
13. Baray, E., & Ojha, N. K. (2021, April). WLAN security protocols and WPA3 security approach measurement through aircrack-ng technique. In 2021 5th International conference on computing methodologies and communication (ICCMC) (pp. 23-30). IEEE.
14. Y. A. Khan, U. Khalil, H. Khan, A. Uddin, S. Ahmed, "Power flow control by unified power flow controller",sss Engineering, Technology & Applied Science Research., vol. 9, no. 2, pp. 3900-3904, Feb. 2019
15. H. Khan, I. Uddin, A. Ali, M. Husain, "An Optimal DPM Based Energy-Aware Task Scheduling for Performance Enhancement in Embedded MPSoC", Computers, Materials & Continua., vol. 74, no. 1, pp. 2097-2113, Sep. 2023
16. Khan, S., Ullah, I., Khan, H., Rahman, F. U., Rahman, M. U., Saleem, M. A., ... & Ullah, A. (2024). Green synthesis of AgNPs from leaves extract of Saliva Sclarea, their characterization, antibacterial activity, and catalytic reduction ability. Zeitschrift für Physikalische Chemie, 238(5), 931-947.
17. S. Khan, I. Ullah, H. Khan, F. U. Rahman, M. U. Rahman, M. A. Saleem, A. Ullah, "Green synthesis of AgNPs from leaves extract of Salvia Sclarea, their characterization, antibacterial activity, and catalytic reduction ability", Zeitschrift für Physikalische Chemie., vol. 238, no. 5, pp. 931-947, May. 2024
18. H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Dec. 2018
19. Waleed, A. Ali, S. Tariq, G. Mustafa, H. Sarwar, S. Saif, I. Uddin, "An Efficient Artificial

Intelligence (AI) and Internet of Things (IoT's) Based MEAN Stack Technology Applications", Bulletin of Business and Economics (BBE)., vol. 13, no. 2, pp. 200-206, July. 2024

20. Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.
21. Noor, A. Ilyas, Z. Javaid, H. Khan, "Framing a Knowledge Domain Visualization on Green Human Resource Management: A Bibliometric Analysis from 2008-2022", Pakistan Journal of Humanities and Social Sciences., vol. 11, no. 4, pp. 4200-4212, Aug. 2023
22. M. Gondal, Z. Hameed, M. U. Shah, H. Khan, "Cavitation phenomenon and its effects in Francis turbines and amassed adeptness of hydel power plant", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-9, Mar. 2019
23. Liang, Y., Ur Rahman, S., Shafaqat, A., Ali, A., Ali, M. S. E., & Khan, H. (2024). Assessing sustainable development in E-7 countries: technology innovation, and energy consumption drivers of green growth and environment. Scientific Reports, 14(1), 28636.
24. U. Hashmi, S. A. ZeeshanNajam, "Thermal-Aware Real-Time Task Schedulabilty test for Energy and Power System Optimization using Homogeneous Cache Hierarchy of Multi-core Systems", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 4, pp. 442-452, Mar. 2023
25. Y. A. Khan, F. Khan, H. Khan, S. Ahmed, M. Ahmad, "Design and Analysis of Maximum Power Point Tracking (MPPT) Controller for PV System", Journal of Mechanics of Continua and Mathematical Sciences., vol. 14, no. 1, pp. 276-288, May. 2019
26. Ali, M., Khan, H., Rana, M. T. A., Ali, A., Baig, M. Z., Rehman, S. U., & Alsaawy, Y. (2024). A Machine Learning Approach to Reduce Latency in Edge Computing for IoT Devices. Engineering, Technology & Applied Science Research, 14(5), 16751-16756.
27. Khan, A. Yasmeen, S. Jan, U. Hashmi, "Enhanced Resource Leveling Indynamic Power Management Techniqueof Improvement In Performance For Multi-Core Processors" ,Journal of Mechanics of Continua and Mathematical Sciences., vol. 6, no. 14, pp 956-972, Sep. 2019
28. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, "Offline Earliest Deadline first Scheduling based Technique for Optimization of Energy using STORM in Homogeneous Multi-core Systems", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 125-130, Oct. 2018
29. Akmal, I., Khan, H., Khushnood, A., Zulfiqar, F., & Shahbaz, E. (2024). An Efficient Artificial Intelligence (AI) and Blockchain-Based Security Strategies for Enhancing the Protection of Low-Power IoT Devices in 5G Networks. Spectrum of engineering sciences, 2(3), 528-586.
30. H. Khan, M. U. Hashmi, Z. Khan, R. Ahmad, A. Saleem, "Performance Evaluation for Secure DES-Algorithm Based Authentication & Counter Measures for Internet Mobile Host Protocol", IJCSNS Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 181-185, July. 2018
31. Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.
32. Khan, A. Ali, S. Alshmrany, "Energy-Efficient Scheduling Based on Task Migration Policy Using DPM for Homogeneous MPSoCs", Computers, Materials & Continua., vol. 74, no. 1, pp. 965-981, Apr. 2023
33. Fakhar, M. H., Baig, M. Z., Ali, A., Rana, M. T. A., Khan, H., Afzal, W., ... & Albouq, S. (2024). A Deep Learning-based Architecture for Diabetes Detection, Prediction, and

Classification. Engineering, Technology & Applied Science Research, 14(5), 17501-17506.

34. Shah, S. Ahmed, K. Saeed, M. Junaid, H. Khan, "Penetration testing active reconnaissance phase–optimized port scanning with nmap tool", In 2019 2nd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-6, Nov. 2019
35. Y. A. Khan, "A GSM based Resource Allocation technique to control Autonomous Robotic Glove for Spinal Cord Implant paralysed Patients using Flex Sensors", Sukkur IBA Journal of Emerging Technologies., vol. 3, no. 2, pp. 13-23, Feb. 2020
36. Y. A. Khan, "A high state of modular transistor on a 105 kW HVPS for X-rays tomography Applications", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 1-6, Jun. 2019
37. Khan, S. Ahmad, N. Saleem, M. U. Hashmi, Q. Bashir, "Scheduling Based Dynamic Power Management Technique for offline Optimization of Energy in Multi Core Processors", Int. J. Sci. Eng. Res., vol. 9, no. 12, pp. 6-10, Dec. 2018
38. Nasir, M. S., Khan, H., Qureshi, A., Rafiq, A., & Rasheed, T. (2024). Ethical Aspects In Cyber Security Maintaining Data Integrity and Protection: A Review. Spectrum of engineering sciences, 2(3), 420-454.
39. Y. A. Khan, "Enhancing Energy Efficiency in Temperature Controlled Dynamic Scheduling Technique for Multi Processing System on Chip", Sukkur IBA Journal of Emerging Technologies., vol. 2, no. 2, pp. 46-53, Jan. 2019
40. Khan, K. Janjua, A. Sikandar, M. W. Qazi, Z. Hameed, "An Efficient Scheduling based cloud computing technique using virtual Machine Resource Allocation for efficient resource utilization of Servers", In 2020 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-7, Apr. 2020
41. Hassan, H. Khan, I. Uddin, A. Sajid, "Optimal Emerging trends of Deep Learning Technique for Detection based on Convolutional Neural Network", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 264-273, Nov. 2023
42. Khan, Q. Bashir, M. U. Hashmi, "Scheduling based energy optimization technique in multiprocessor embedded systems", In 2018 International Conference on Engineering and Emerging Technologies (ICEET), IEEE., pp. 1-8, Sep. 2018
43. Javed, M. A., Anjum, M., Ahmed, H. A., Ali, A., Shahzad, H. M., Khan, H., & Alshahrani, A. M. (2024). Leveraging Convolutional Neural Network (CNN)-based Auto Encoders for Enhanced Anomaly Detection in High-Dimensional Datasets. Engineering, Technology & Applied Science Research, 14(6), 17894-17899.
44. Y. A. Khan, M. Ibrahim, M. Ali, H. Khan, E. Mustafa, "Cost Benefit Based Analytical Study of Automatic Meter Reading (AMR) and Blind Meter Reading (BMR) used by PESCO (WAPDA)", In 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), IEEE., pp. 1-7, Aug. 2020
45. Rahman, M. U., Khan, S., Khan, H., Ali, A., & Sarwar, F. (2024). Computational chemistry unveiled: a critical analysis of theoretical coordination chemistry and nanostructured materials. Chemical Product and Process Modeling, 19(4), 473-515.
46. Naz, H. Khan, I. Ud Din, A. Ali, and M. Husain, "An Efficient Optimization System for Early Breast Cancer Diagnosis based on Internet of Medical Things and Deep Learning", Eng. Technol. Appl. Sci. Res., vol. 14, no. 4, pp. 15957–15962, Aug. 2024
47. Khan, I. Ullah, M. U. Rahman, H. Khan, A. B. Shah, R. H. Althomali, M. M. Rahman, "Inorganic-polymer composite electrolytes: basics, fabrications, challenges and future perspectives", Reviews in Inorganic Chemistry., vol. 44, no. 3, pp. 1-2, Jan. 2024
48. Naveed, A., Khan, H., Imtiaz, Z., Hassan, W., & Fareed, U. (2024). Application and Ethical

Aspects of Machine Learning Techniques in Networking: A Review. Spectrum of engineering sciences, 2(3), 455-501.

49. Sarwar, H. Khan, I. Uddin, R. Waleed, S. Tariq, "An Efficient E-Commerce Web Platform Based on Deep Integration of MEAN Stack Technologies", Bulletin of Business and Economics (BBE)., vol. 12, no. 4, pp. 447-453, Jun. 2023
50. Sebbar, A., Boulahya, S. E., Mezzour, G., & Boulmalf, M. (2016, May). An empirical study of wifi security and performance in morocco-wardriving in rabat. In 2016 International Conference on Electrical and Information Technologies (ICEIT) (pp. 362-367). IEEE.
51. Sagers, G., Hosack, B., Rowley, R. J., Twitchell, D., & Nagaraj, R. (2015, January). Where's the security in WiFi? An argument for industry awareness. In 2015 48th Hawaii international conference on system sciences (pp. 5453-5461). IEEE.
52. Zhang, S., Venkatnarayan, R. H., & Shahzad, M. (2020, December). A wifi-based home security system. In 2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS) (pp. 129-137). IEEE.
53. Hooper, M., Tian, Y., Zhou, R., Cao, B., Lauf, A. P., Watkins, L., ... & Alexis, W. (2016, November). Securing commercial WiFi-based UAVs from common security attacks. In MILCOM 2016-2016 IEEE Military Communications Conference (pp. 1213-1218). IEEE.