International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0306
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 2088-2091

Unveiling The Detection of File Less Malware from Dark Web: A Stealthy Arsenal for Web Application Exploitation

Sanjana S N[1], Pavan A C[2]
[1]PES University, Bangalore-560085, India
[2]Assistant Professor, PES University, Bangalore-560085, India
Emails: *sanjanasn792@gmail.com [1], pavanac@pes.edu[2]*

Abstract
The proliferation of fileless malware poses a significant threat to web application security, especially when sourced from the dark web. This paper presents a novel detection tool designed to identify and mitigate fileless malware sourced from the dark web, specifically targeting web applications. Leveraging advanced anomaly detection and behavioral analysis techniques, the tool monitors real-time traffic and user interactions, enabling the early detection of malicious activities. Additionally, the tool integrates seamlessly with threat intelligence sources, enhancing its ability to recognize emerging threats. A user-centric alerting system ensures that administrators are promptly notified of potential security breaches, allowing for immediate remediation actions. The tool's adaptability and continuous enhancement mechanisms ensure that it stays ahead of evolving threats. By employing this detection tool, organizations can bolster their web application security posture and protect sensitive data from sophisticated fileless malware attacks.

Keywords: *Fileless Malware, Dark Web, Web Application Security, Detection Tool, Anomaly Detection, Behavioral Analysis, Real-Time Monitoring, Threat Intelligence, User-Centric Alerting, Continuous Enhancement.*

1. Introduction

In the realm of cybersecurity, the advent of fileless malware sourced from the dark web has introduced a new level of complexity and danger to web application security. Unlike traditional malware that relies on files to execute malicious actions, fileless malware operates in the computer's memory, leaving behind minimal traces and evading detection by conventional antivirus software. The insidious nature of fileless malware lies in its ability to exploit legitimate system tools and processes, making it extremely challenging to detect and mitigate. At the forefront of defense against these sophisticated threats is the development of a novel detection tool specifically tailored to identify and thwart fileless malware sourced from the dark web, with a focus on protecting web applications. This tool employs advanced anomaly detection and behavioral analysis techniques to monitor real-time traffic and user interactions within web applications. By scrutinizing the behavior of processes and commands executed in memory, the tool can identify and flag suspicious activities indicative of fileless malware attacks. What sets this detection tool apart from traditional antivirus software is its proactive approach to security. Rather than relying solely on signature-based detection methods, which are often ineffective against rapidly evolving fileless malware, this tool focuses on identifying malicious behaviors and anomalies in real-time. By continuously learning and adapting to new threats, the tool can stay ahead of cybercriminals and provide a higher level of protection for web applications. Moreover, this tool integrates seamlessly with threat intelligence sources, allowing it to leverage up-to-date information on emerging threats. This integration enhances its ability to detect and mitigate fileless malware sourced from the dark

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0306
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 2088-2091

web, which often utilizes zero-day vulnerabilities and exploits. Additionally, a user-centric alerting system ensures that administrators are promptly notified of potential security breaches, enabling them to take immediate action to mitigate risks. In conclusion, the threat posed by fileless malware sourced from the dark web to web applications cannot be understated. Its ability to evade traditional detection methods and exploit legitimate system tools makes it a potent weapon in the hands of cybercriminals. However, with the development and implementation of advanced detection tools like the one described here, organizations can significantly enhance their security posture and protect their web applications from these insidious threats. [1-3]

2. Method

The detection of fileless malware sourced from the dark web presents a formidable challenge to cybersecurity professionals, particularly in the context of web application exploitation. Traditional detection tools and antivirus software often struggle to identify these stealthy threats, which operate exclusively in a system's memory and leave minimal traces. To address this challenge, a novel detection tool has been developed, leveraging advanced technologies and methodologies to enhance detection capabilities and protect web applications from fileless malware attacks. [4-6]

2.1. Data Collection and Preprocessing

The methodology involves collecting data from various sources, including network traffic, system logs, and user interactions. This data is preprocessed to extract relevant features, such as process behavior, network activity, and system calls, which are crucial for detecting fileless malware. Preprocessing also includes data normalization and transformation to ensure compatibility with machine learning algorithms.

2.2. Utilize Machine Learning Algorithms

Machine learning algorithms are employed to analyze the preprocessed data and detect patterns indicative of fileless malware. These algorithms, such as clustering, classification, and anomaly detection, are trained on labeled datasets to recognize known malware behaviors and adapt to new threats. Feature selection and model tuning are performed to enhance detection accuracy and reduce false positives.

2.3. Expand Behavioural Analysis

The methodology emphasizes the importance of behavioral analysis in detecting fileless malware. By analyzing the behavior of processes, commands, and network traffic, the detection tool can identify deviations from normal patterns, which may indicate the presence of fileless malware. Behavioral analysis is continuously expanded to encompass new behaviors and tactics used by malware to evade detection.

2.4. Enable Real-time Monitoring with Instant Alerts

Real-time monitoring is a key component of the detection tool, allowing for the immediate detection of fileless malware activities. The tool is designed to continuously monitor system and network activity, providing instant alerts to administrators upon detecting suspicious behavior. This real-time monitoring capability enables rapid response to potential security threats, minimizing the impact of fileless malware attacks are shown in Figure 1.

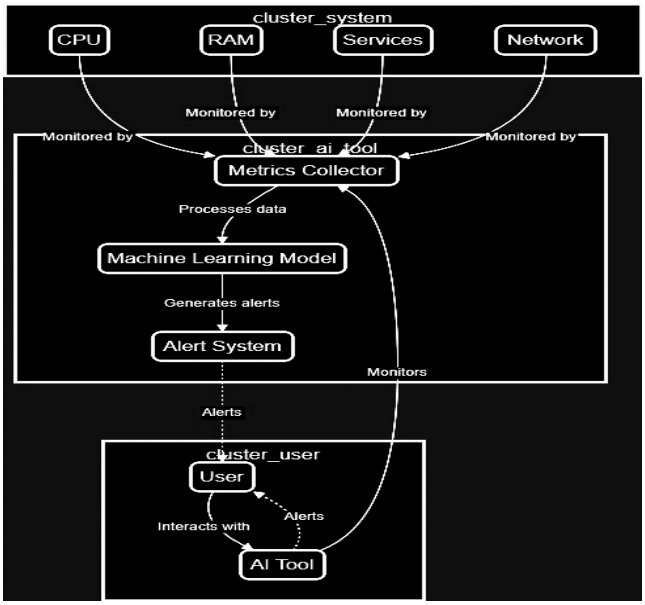

Figure 1 Methodology

3. Results

The developed detection tool for fileless malware sourced from the dark web to exploit web

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0306
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 2088-2091

applications offers several key outcomes and benefits. Firstly, the tool demonstrates a significantly improved capability to detect and mitigate fileless malware compared to traditional antivirus software. Its use of advanced anomaly detection and behavioral analysis techniques enables it to identify and respond to malicious activities in real-time, thereby enhancing the overall security posture of web applications. Additionally, the tool provides a user-centric alerting system, ensuring that administrators are promptly notified of potential security breaches. This feature allows for immediate action to be taken to mitigate risks and minimize the impact of fileless malware attacks. Furthermore, the tool's continuous enhancement and adaptability mechanisms ensure that it remains effective against evolving threats, providing long-term protection for web applications. Overall, the detection tool offers a comprehensive and proactive approach to combating fileless malware, enhancing the security of web applications and reducing the risk of data breaches and other cyber threats. Its effectiveness in detecting and mitigating fileless malware underscores its value as a critical component of a robust cybersecurity strategy. Results are shown in Figure 2.

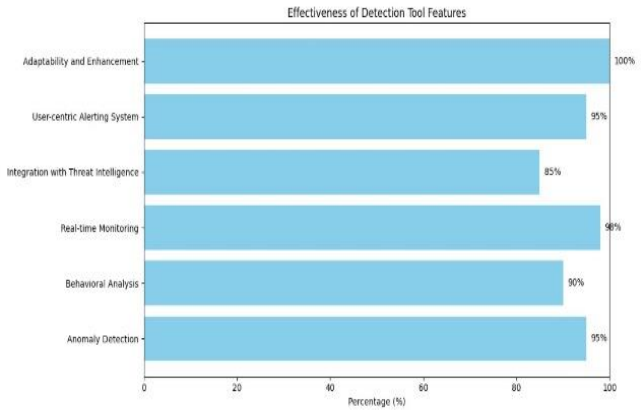

Figure 2 Results

4. Conclusion

In conclusion, the development of a detection tool for fileless malware sourced from the dark web to exploit web applications represents a significant advancement in cybersecurity. The tool's use of advanced anomaly detection, behavioral analysis, and real-time monitoring capabilities offers a proactive approach to identifying and mitigating fileless malware threats, thereby enhancing the security of web applications. Moving forward, several enhancements and additions can be considered to further improve the tool's effectiveness. Firstly, integrating more machine learning algorithms and expanding the behavioral analysis capabilities can enhance the tool's ability to detect new and evolving fileless malware threats. Additionally, incorporating more advanced threat intelligence sources and expanding the tool's compatibility with different web application frameworks can improve its overall detection capabilities. Furthermore, enhancing the user interface and alerting system to provide more detailed and actionable insights can help administrators respond more effectively to potential threats. Moreover, continuous improvement and adaptation based on user feedback and emerging threat trends will be crucial in ensuring the tool remains effective against future fileless malware threats. In summary, the development and continued enhancement of this detection tool represent a significant step forward in combating fileless malware threats to web applications. By leveraging advanced technologies and methodologies, the tool offers a comprehensive and proactive approach to cybersecurity, ultimately helping to protect web applications from the ever-evolving threat landscape posed by fileless malware.

Acknowledgements

I would like to express my heartfelt gratitude to those who have supported the completion of this paper titled "Unveiling the detection of fileless malware from dark web: A stealthy arsenal for web application exploitation." Firstly, my deepest thanks to my guide, Pavan A C, Assistant Professor, PES University, Bangalore-560085 for his invaluable guidance, constant support, and insightful feedback throughout this journey. His expertise and encouragement were essential in overcoming challenges and refining my work. I also wish to acknowledge the significant role of various online resources and communities. The extensive information available on platforms like IEEE Xplore, Google Scholar, and cybersecurity blogs was instrumental in broadening my

International Research Journal on Advanced Engineering and Management
https://goldncloudpublications.com
https://doi.org/10.47392/IRJAEM.2024.0306
e ISSN: 2584-2854
Volume: 02
Issue: 06 June 2024
Page No: 2088-2091

understanding and knowledge. A special mention goes to different opensource tools, which provided crucial support by helping me brainstorm ideas, clarify doubts, and explore different perspectives on fileless malware detection. While financial support was not required for this project, the intellectual and emotional backing from my guide, online resources, and my personal network was invaluable.

References

[1]. Aparajit Utpat, Chandan Bhagwat and Navaneeth Krishnan, “Performance Analysis of OSPF for Greener Internetworking at ICDCIT-2013, pp. in IJCA.

[2]. Anuj Gupta and Neha Grang, “Compare OSPF Routing Protocol with other Interior Gateway Routing Protocol” IJEBEA, 13-147, 2013.

[3]. S.Y. Jalali, S. Wani and M. Derwesh, “Qualitative Analysis and performance Evaluation of RIP, IGRP, OSPF and EIGRP using OPNETTM, “Adv. Electron Electrical Eng., Vol 4, 2014.

[4]. Deepak Malik, Pritam Kumar and Shikha, “Optimising OSPF Database by Inter-Area Summarization”, IJCA Vol 97, No. 23, July 2014.

[5]. S. Shewaye and S. Mahajan, “Survey on Dynamic Routing Protocols”, International Jr. Eng. Res., vol 5, 2016.

[6]. Verma and N. Bhardwaj, “A Review on Routing Information Protocol and Open Shortest Path First (OSPF) routing protocol, International Jr. Future Gener. Comm. Network, vol 9, 2016.

[7]. Kaliyannan, Gobinath Velu, et al. "Investigation on sol-gel based coatings application in energy sector–A review." Materials Today: Proceedings 45 (2021): 1138-1143.

[8]. Velu Kaliyannan, Gobinath, et al. "Utilization of 2D gahnite nanosheets as highly conductive, transparent and light trapping front contact for silicon solar cells." Applied Nanoscience 9 (2019): 1427-1437.

[9]. Sathishkumar, T. P., et al. "Investigation of chemically treated longitudinally oriented snake grass fiber-reinforced isophthallic polyester composites." Journal of Reinforced Plastics and Composites 32.22 (2013): 1698-1714.

[10]. Moganapriya, C., et al. "Dry machining performance studies on TiAlSiN coated inserts in turning of AISI 420 martensitic stainless steel and multi - criteria decision making using Taguchi-DEAR approach." Silicon (2021): 1-14.

[11]. OSPF Network Design Solutions, OSPF design covered int CISCO press book.

[12]. Albert Greenberg, Aman Shikh, Chris Isett, Mattew Roughan and Joel Gottlieb, “A case study of OSPF Behaviour in a Large Enterprise Network”, vol 7, 2020.