IJARETY

International Journal of Advanced Research in Education and TechnologY (IJARETY)

Volume 12, Issue 1, January-February 2025

Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com

International Journal of Advanced Research in Education and TechnologY(IJARETY)

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January-February 2025 ||

DOI:10.15680/IJARETY.2025.1201003

Analyzing and Mitigating Malware: Techniques, Challenges, and Future Directions

Mario Geraldy Foris, Stephanus Antonius Ananda, Agustinus Noertjahyana

Department of Informatics, Petra Christian University, Indonesia

ABSTRACT: This paper aims to analyze malware, particularly modern malware, focusing on how malware behaves on the host, its propagation, its functions, and the IoCs of each malware. Given the increasing prevalence of cyber-attacks in cyberspace, there is a need to analyze new malware, especially in terms of how to mitigate malware that has not yet infected or is already present in the host computer. Malware has already become a threat to internet users, but in an era where everyone has a device, this threat becomes more "real," especially with the numerous news stories of Indonesians being affected by malware, such as phishing websites. This paper will analyze the obtained malware data and then compare it to mitigate the threat of malware.

KEYWORDS: Malware, Malware Analysis, Malware Mitigation

I. INTRODUCTION

Malware is a term derived from combining the words “malicious” and “software.” It refers to software designed to execute tasks on computer systems without the user’s consent or intent. Malware is typically created to interfere with or halt operations, collect sensitive data, or gain unauthorized access to system resources [1].

The threat of malware is increasingly apparent today, highlighted by news about phishing victims in Indonesia and a data breach at Kemenkominfo in 2024, causing public panic about cyber threats. On the other hand, cybersecurity personnel, especially malware analysts, continually strive to combat the cybercrime that occurs daily. This situation raises questions about how to eliminate or mitigate the threat of malware that is widely spreading in cyberspace. A digitally connected world comes with unseen threats to cyberspace, governments, actors from business, and individuals are identifiable targets for cyber criminals who are promoting their activities due to technological changes. The rapid expansion of digital technology has significantly transformed society, influencing how we work, live, and interact. This transformation has opened up new opportunities for innovative businesses and economic advancement. However, it has also empowered attackers, leading to increasingly sophisticated and widespread cyberattacks. From high-profile incidents like ransomware and phishing to intricate cases of cyber espionage and warfare, the scale and severity of these threats have grown dramatically, posing substantial challenges to cybersecurity professionals and organizations worldwide [2].

One approach as a malware analyst involves analyzing the IoCs, behavior, and signatures of malware circulating on the internet. With this method, it's possible to stop both old and new malware from entering or damaging the system on a device. However, this becomes a challenge on its own due to modern malware that uses evasive techniques to hide from malware analysts. Despite ongoing advancements in cybersecurity mechanisms and their continuous development, malware remains one of the most effective threats in cyberspace. Malware analysis incorporates techniques from various disciplines, such as program and network analysis, to examine malicious samples and gain deeper insight into their behavior and evolution. In the persistent battle between malware developers and analysts, improvements in security technology are often swiftly countered with evasion techniques. The effectiveness of new defense measures often hinges on the properties they target. For instance, a detection rule relying on the MD5 hash of a known malware can be easily bypassed using basic obfuscation methods or more sophisticated techniques like polymorphism and metamorphism [3]. In this context, the paper will analyze malware circulating in cyberspace. The malware to be analyzed is of the PE (Portable Executable) file type. Data from the malware, such as IoCs, behavior, and signatures, will be collected and used as data for mitigating the threat from circulating malware.

II. LITERATURE REVIEW

The primary issue addressed in this research is the widespread ownership of computers and laptops in modern households. Unfortunately, many users, particularly those with limited technical knowledge, are vulnerable to cyber

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January-February 2025 ||

DOI:10.15680/IJARETY.2025.1201003

threats. Attackers often exploit security weaknesses in these devices or manipulate users into downloading malicious files—such as cracked software—or visiting untrusted websites, leading to malware infections. Depending on its type, malware can cause significant harm to victims, including financial loss or reputational damage due to data breaches and unauthorized access.

Malware exists in various forms and can be categorized based on its behavior and impact. These classifications are not mutually exclusive, as some malware types exhibit characteristics of multiple categories [4]. The following are some of the most prevalent types of malwares:

Virus: A virus is a self-replicating computer program that embeds itself into other applications or files. While often hidden within seemingly harmless software, it can execute malicious actions such as corrupting data, disrupting system functionality, or spreading to other devices [5].

Trojan: A Trojan horse is one of the most dangerous forms of malware. It masquerades as a legitimate application to deceive users into installing it. Once executed, it grants attackers unauthorized access to the infected system. Trojans are commonly used for stealing financial information or deploying additional malware, such as ransomware [6].

Spyware: Spyware is designed to secretly monitor user activity and collect sensitive information, such as banking credentials and login details. It can spread through software vulnerabilities, be bundled with legitimate applications, or be delivered via Trojans [7].

Adware: Adware is a type of software that tracks user behavior and displays targeted advertisements. While not inherently malicious, it can compromise system security by redirecting users to unsafe websites or containing spyware and Trojans. Additionally, excessive adware can significantly slow down system performance. Given that not all adware is harmful, security software capable of detecting and managing these programs is essential [8].

Keyloggers: Keyloggers are a form of spyware that record keystrokes to track user activity. Although they have legitimate applications, such as employee monitoring or parental supervision, they are frequently exploited for malicious purposes. Cybercriminals use keyloggers to steal sensitive data, including passwords and financial information, often deploying them through phishing attacks or malicious downloads [9].

Ransomware: Ransomware encrypts files stored on a user's device and demands payment in exchange for a decryption key. Although it does not typically block access to the computer itself, it renders all affected data inaccessible until the ransom is paid [10].

Understanding these malware types is crucial for implementing effective cybersecurity measures to mitigate the risks they pose.

III. METHODOLOGY

The malware analysis in this study is conducted using virtualization. This approach allows malware to be examined in a controlled environment, minimizing the risk of infecting the host system. According to previous research [11], one of the effective methods for combating malware is using a virtual environment within a network device or host agent. Therefore, the virtualization techniques used in this study include:

3.1 Virtual Machine-Based Analysis

A virtual machine (VM) provides an isolated environment for analyzing malware, ensuring that malicious code can be executed without affecting the host system. One of the most used virtual machines for malware analysis is FlareVM. FlareVM is a collection of software installation scripts for Windows systems, enabling users to easily set up and maintain a reverse engineering environment within a virtual machine.

FLARE-VM was specifically designed to address the challenge of curating reverse engineering tools and relies on two key technologies: Chocolatey and Boxstarter. Chocolatey is a Windows-based NuGet package management system that allows for the automated installation and configuration of various tools. Boxstarter extends Chocolatey by automating software deployment, facilitating the creation of reproducible Windows environments for malware analysis [12].

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January-February 2025 ||

DOI:10.15680/IJARETY.2025.1201003

3.2 Sandboxing

Another method used in malware analysis is sandboxing, where a suspicious file is uploaded to an online sandbox service for examination. This technique is widely used due to its convenience, as sandbox environments come pre-equipped with analytical tools that provide comprehensive information about the malware, including its type, Indicators of Compromise (IoCs), behavior, and attack patterns.

Malware sandbox systems play a crucial role in security applications and are widely integrated into intrusion detection systems, forensic analysis pipelines, automated reverse engineering tools, and threat intelligence services [13]. These systems help cybersecurity professionals detect, analyze, and mitigate malware threats efficiently.

3.3 Limitations

One of the primary challenges in malware analysis is the presence of evasive malware, which employs sophisticated techniques to avoid detection. As stated in previous research [3], early malware was relatively simple and easily detectable, often causing minor disruptions by displaying messages or modifying system behavior. However, modern malware has evolved significantly, becoming more sophisticated and financially motivated.

A particularly severe form of malware is ransomware, which encrypts victims' files and demands payment for decryption. Additionally, governments and state-sponsored actors have developed Advanced Persistent Threats (APT) for espionage, sabotage, and intelligence gathering [14]. The increasing complexity of modern malware makes its analysis more challenging, requiring advanced skills and specialized tools.

Furthermore, the use of virtual machines (VMs) in malware analysis presents certain drawbacks. According to prior studies [15], while VMs can be easily deployed and discarded after completing an analysis, they lack an efficient mechanism for transferring safe changes back to the host system. If no malicious activity is detected, users must manually replicate their work in the actual workspace, leading to inefficiencies in the workflow.

Despite these limitations, virtualization and sandboxing remain essential techniques for malware analysis, providing a safe and effective environment for studying malicious software.

IV. RESULT AND DISCUSSION

The malware analyzed in this study consists of samples commonly found circulating on the internet, including those available in repositories such as The Zoo on GitHub. The selected malware samples represent different types and functionalities, providing a comprehensive analysis of various malware behaviors. The chosen malware includes:

- Zeus Banking Trojan
- Trojan Agent Tesla
- WannaCry Ransomware
- Thanos Ransomware
- Trojan Petya
- Raccoon Stealer

The analysis of each malware sample is detailed as follows:

Zeus Banking Trojan

Zeus Banking Trojan is a well-known banking malware designed to steal sensitive user information. Its primary functions include:

Keylogging: Captures user keystrokes, enabling attackers to obtain credentials and other sensitive data.

Browser Injection: Injects malicious scripts into web browsers to extract login information, particularly targeting banking credentials.

Trojan Agent Tesla

Agent Tesla is a widely used Remote Access Trojan (RAT) with extensive credential-stealing capabilities. Its key functions include:

Credential Theft: Extracts sensitive information from browsers, email clients, FTP/SCP clients, remote administration tools, VPN applications, and instant messaging services.

Keylogging: Records user keystrokes to capture login credentials and other confidential data.

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January-February 2025 ||

DOI:10.15680/IJARETY.2025.1201003

WannaCry Ransomware & Thanos Ransomware
Both WannaCry and Thanos operate as ransomware, with their primary function being:
Data Encryption & Ransom Demand: Encrypts user files and demands payment (typically in cryptocurrency) for the decryption key.

Trojan Petya
Petya is a ransomware-type Trojan with a destructive payload. Its functionalities include:
System Disruption: Modifies the system's Master Boot Record (MBR), rendering the device unbootable.
File Encryption & Ransom Demand: Encrypts store files and demands payment for decryption, similar to traditional ransomware.

Raccoon Stealer
Raccoon Stealer is an information-stealing malware designed to harvest user credentials. Its main objectives include:
Credential Theft: Extracts autofill data from web browsers, allowing attackers to access stored login credentials.
Cryptocurrency Wallet Theft: Targets and exfiltrates cryptocurrency wallets from infected systems.
The results highlight the diverse techniques employed by different malware types, reinforcing the need for advanced security measures to detect and mitigate these threats effectively.

V. CONCLUSION AND FUTURE WORK

The malware analyzed in this study consists of samples sourced from publicly available repositories such as GitHub and MalwareBazaar. While these samples may not fully represent the most recent malware variants, they still employ evasive techniques and attack methods commonly found in modern malware. Despite continuous modifications in malware behavior, the underlying techniques remain relevant for security analysis.

- To mitigate the risks associated with malware, general users can adopt several preventive measures, including:
- Avoiding the download of suspicious files (e.g., cracked software).
- Refraining from visiting potentially malicious websites.
- Regularly updating Windows Defender and the operating system.
- Conducting periodic system checks.
- Installing reputable antivirus software such as Kaspersky, which offers malware scanning, phishing protection, and ransomware detection.
- Using password managers like Bitwarden to protect against keylogger-based malware.
- Backing up important files to cloud storage solutions such as Google Drive.

Additionally, more advanced security measures, such as implementing Security Information and Event Management (SIEM) systems, can enhance malware detection and response capabilities. However, SIEM solutions typically require significant system resources and a higher level of technical expertise, making them more suitable for users with advanced computing knowledge and capable hardware.

By adopting these preventive strategies, users can significantly reduce the risk of malware infections and enhance overall cybersecurity resilience.
The landscape of malware threats is expected to remain dynamic, with threat actors continuously developing more sophisticated techniques to evade detection. As a result, malware analysts must persistently analyze newly emerging threats, making it unlikely that malware mitigation will ever reach 100% effectiveness. However, implementing robust preventive measures remains the most viable strategy for reducing the risks associated with malware infections.

One promising approach to enhancing cybersecurity is the integration of artificial intelligence (AI)-based antivirus software. AI-driven solutions aim to improve malware detection accuracy while minimizing false positives. With the rapid evolution of cyber threats, machine learning (ML) and deep learning have become essential tools for strengthening security frameworks. By leveraging large datasets and identifying patterns that traditional methods might overlook, AI-powered cybersecurity systems offer a more proactive and adaptive approach to threat detection and mitigation.

The incorporation of neural networks and deep learning algorithms in cybersecurity has significantly enhanced the ability to detect and analyze malware. These AI-driven methods allow for real-time threat assessment and continuous learning, enabling security systems to adapt to emerging threats more effectively. As cybercriminals refine their

| ISSN: 2394-2975 | www.ijarety.in| | Impact Factor: 7.394| A Bi-Monthly, Double-Blind Peer Reviewed & Referred Journal |

|| Volume 12, Issue 1, January-February 2025 ||

DOI:10.15680/IJARETY.2025.1201003

techniques, ongoing advancements in AI and ML will play a crucial role in fortifying cybersecurity defenses and mitigating future malware risks [16].

REFERENCES

[1] A. Pektaş and T. Acarman, "A dynamic malware analyzer against virtual machine aware malicious software," Secur. Commun. Netw., vol. 7, no. 12, pp. 2245–2257, Dec. 2014, doi: 10.1002/sec.931.
[2] V. Kolluri, "AN EXTENSIVE INVESTIGATION INTO GUARDIANS OF THE DIGITAL REALM: AI-DRIVEN ANTIVIRUS AND CYBER THREAT INTELLIGENCE," vol. 2, no. 11, 2015.
[3] D. Ucci, L. Aniello, and R. Baldoni, "Survey of machine learning techniques for malware analysis," Comput. Secur., vol. 81, pp. 123–147, Mar. 2019, doi: 10.1016/j.cose.2018.11.001.
[4] Department of Computer Science, Virtual University of Pakistan and R. Tahir, "A Study on Malware and Malware Detection Techniques," Int. J. Educ. Manag. Eng., vol. 8, no. 2, pp. 20–30, Mar. 2018, doi: 10.5815/ijeme.2018.02.03.
[5] Anusmita Ray and Dr. Asoke Nath, "Introduction to Malware and Malware Analysis: A brief overview," Int. J. Adv. Res. Comput. Sci. Manag. Stud..
[6] "What is Malware? Malware Definition, Types and Protection," Malwarebytes. Accessed: Nov. 12, 2024. [Online]. Available: https://www.malwarebytes.com/malware
[7] "Types of Malware & Malware Examples," /. Accessed: Dec. 14, 2024. [Online]. Available: https://www.kaspersky.com/resource-center/threats/types-of-malware
[8] "What Is Malware? - Definition and Examples," Cisco. Accessed: Dec. 14, 2024. [Online]. Available: https://www.cisco.com/site/us/en/learn/topics/security/what-is-malware.html
[9] "12 Types of Malware + Examples That You Should Know | CrowdStrike," CrowdStrike.com. Accessed: Dec. 14, 2024. [Online]. Available: https://www.crowdstrike.com/en-us/cybersecurity-101/malware/types-of-malware/
[10] O. Or-Meir, N. Nissim, Y. Elovici, and L. Rokach, "Dynamic Malware Analysis in the Modern Era—A State of the Art Survey," ACM Comput. Surv., vol. 52, no. 5, pp. 1–48, Sep. 2020, doi: 10.1145/3329786.
[11] R. Rehman, D. G. C. Hazarika, and G. Chetia, "MALWARE THREATS AND MITIGATION STRATEGIES: A SURVEY," . Vol., vol. 29, 2005.
[12] mandiant/flare-vm. (Nov. 26, 2024). PowerShell. MANDIANT. Accessed: Nov. 27, 2024. [Online]. Available: https://github.com/mandiant/flare-vm
[13] O. Alrawi, M. Y. Wong, A. Avgetidis, K. Valak, and K. Karak, "SoK: An Essential Guide For Using Malware Sandboxes In Security Applications: Challenges, Pitfalls, and Lessons Learned".
[14] M. N. Alenezi, H. K. Alabdulrazzaq, A. A. Alshaher, and M. M. Alkharang, "Evolution of Malware Threats and Techniques: a Review," Int. J. Commun. Netw. Inf. Secur. IJCNIS, vol. 12, no. 3, Apr. 2022, doi: 10.17762/ijcnis.v12i3.4723.
[15] Zhiyong Shan, Xin Wang, and Tzi-cker Chiueh, "Malware Clearance for Secure Commitment of OS-Level Virtual Machines," IEEE Trans. Dependable Secure Comput., vol. 10, no. 2, pp. 70–83, Mar. 2013, doi: 10.1109/TDSC.2012.88.
[16] J. N. Chukwunweike, P. A. Ayodele, O. Obasuyi, A. Oluwamayowa, and A. Samson, "AI AND DEEP CYCLE PREDICTION: ENHANCING CYBERSECURITY WHILE SAFEGUARDING DATA PRIVACY AND INFORMATION INTEGRITY," Int. J. Res. Publ. Rev., vol. 5, no. 8, pp. 3199–3207, Aug. 2024, doi: 10.55248/gengpi.5.0824.2403.

International Journal of Advanced Research in Education and Technology

ISSN: 2394-2975 Impact Factor: 7.394

www.ijarety.in editor.ijarety@gmail.com