SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V11I12P102

Volume 11 Issue 12, 12-19, December 2024
© 2024 Seventh Sense Research Group®

Review Article

In-depth Malware Behaviour Analysis: Network and Registry Changes in an Isolated Windows Environment

Abdullahi Mohamud Osoble[1*], Adam Muhudin[1], Yahye Abukar Ahmed[1], Osman Diriye Hussein[2], Abdirahman Abdullahi Omar[1]

[1]*Faculty of Computing, SIMAD University, Mogadishu, Somalia.*
[2]*Faculty of Engineering, SIMAD University, Mogadishu, Somalia.*

[*]*Corresponding Author : osoble252@gmail.com*

Received: 08 October 2024 Revised: 11 November 2024 Accepted: 02 December 2024 Published: 30 December 2024

Abstract *- This paper analyzes the malware variant of samples.exe and its impact on a Windows 10 virtual machine. The analysis employs Process Monitor (ProcMon) and Regshot as key tools to observe and document malware behavior. ProcMon tracks real-time events such as registry manipulations and DNS configuration changes, while Regshot captures and compares pre- and post-infection registry states. As sophisticated information-tracking utilities, like ProcMon and Regshot, have records at every step of malware operation, some obvious changes to system registry and network settings have been noticed. Key findings: This virus changes DNS settings. This would have an impact on traffic routing into malicious websites; the turning off of the real-time protection of the Windows Defender, a normal practice seen in this kind of virus for avoiding detection and hence assured persistence. Still, more modification in registry locations, especially related to Windows Error Reporting and Group Policy, hints at the big malware plan to destroy system policies and hide within them. The above steps have uncovered how strategic malware can threaten the system's stability and network integrity by severely compromising its security. In this regard, research overemphasizes the desperate need for capable detection mechanisms and proactive security measures that help overcome this ever-emerging threat in present and modern computer environments.*

Keywords *- Malware analysis, Registry modifications, DNS settings, ProcMon, Regshot.*

1. Introduction

Malicious software, or malware, is designed to disturb systems, help unauthorized access, or steal sensitive information. In fact, during these years, the rampant presence of malware, such as viruses, worms, Trojans, and rootkits, has been a big challenge for cybersecurity professionals regarding detection and remediation [1].

According to IBM (2023), the average cost of a data breach worldwide in 2023 was $4.45 million, demonstrating cybercrime's deep financial and operational impact. Therefore, global annual costs attributed to cybercrime by 2024 are projected to reach $9.5 trillion (eSentire) [2]. Given such alarming news, it is surprising how many organizations still do not adequately spend on security measures, so these critical systems are increasingly exposed to more sophisticated threats. Cybercrimes cost the globe over US$600 billion annually, or 0.8% of the GDP (Mordor Intelligence, 2024). Furthermore, it takes about 277 days to handle the fallout from a cyberattack (IBM 2022); of the companies that have had several data breaches, just 51% have raised their security spending, while 57% have passed on the event costs to their customers (IBM 2023) [2].

Existing malware detection methods struggle to keep up with evolving threats [4]. Dynamic analysis offers valuable insights into malware activity but lacks a comprehensive view of transient (e.g., network) and persistent (e.g., registry) changes. Additionally, signature-based methods are less effective against polymorphic and metamorphic malware, which adapt to evade detection. These limitations reveal a gap in understanding and mitigating how malware compromises system integrity.

1.1. The Evolution of Malware Throughout History

Since the advent of computers, programmers have been developing programs that alter their behavior, with some being malicious [17]. This overview provides a glimpse into the history of malware, highlighting significant milestones [3].

1.2. Understanding Malware: Analysis, Detection, and the Role of Network Traffic

Malware refers to harmful software that purposefully performs detrimental actions [19]. Harmful programs are divided into various categories based on their behaviors and how they affect processes, such as viruses, trojan horses,

This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/)

rootkits, backdoors, spyware, logic bombs, adware, and ransomware are a few examples [19]. Computer systems are attacked for various reasons, including destroying computer resources, obtaining financial gain, stealing private data, exploiting computational resources [18], and disabling services for the system [4].

1.2.1. The General Impact of Malware

Malware has a wide-ranging impact, causing significant financial losses, operational disruptions, and data breaches [20]. Organizations face substantial costs from recovery efforts, fines, and lost revenue. Malware can halt operations, affecting everything from business functions to essential public services [5].

Additionally, data breaches resulting from malware lead to the theft or loss of sensitive information [21], with consequences like identity theft and financial fraud. The negative impacts ripple through the company's brand, often causing long-term loss of consumer confidence [22]. This might be very adverse and stresses the tremendous need for and urgency of cybersecurity protection [5].

1.2.2. The Future of Malware and Emerging Threats

The future malware with AI-generated attacks is on the rise, as will be noted in [23]. These AI attacks can adapt and learn from defenses, making detecting and stopping these attacks much harder [24]. Cybersecurity must also evolve to stay capable against such smarter attacks. For more about this, read studies carried out on AI-driven malware [6].

Fileless malware is an up-and-coming threat since it does not leave a trace in the hard drive, making detection very hard [25]. This malware resides in one computer's RAM, evading many traditional security measures. As this threat grows, research in new methodologies to detect and protect from it is very much needed [26].

1.2.3. Problem Statement

System security is seriously in danger due to the growing sophistication of malware assaults, significantly when changing important system settings and turning off protection features [8]. This study examines the effects of a particular virus on a Windows-based machine. The malware is known as virus samples.exe [9].

The present analysis reveals serious tampering with registry keys, system policies, and security settings by comparing the system states before and after the infection in minute detail [9]. Most specifically, this malware changes DNS settings. It turns off the real-time protection of Windows Defender [11], thus compromising the integrity of the system's network [12] and further exposing it to other kinds of threats [13]. Remediation should be made to diminish the potential for ongoing unauthorized access and possible data breaches [14].

In fact, the whole analysis will draw from the observations of both registry state comparisons, and Procmon captures [16], validating the sequence of malicious actions with implications for system security [15].

2. Literature Review

The growing sophistication of malware has posed significant challenges in its detection and prevention. Over the years, researchers have explored many approaches to understanding malware, including but not limited to its classification, evolution, and detection methods. Despite advancements, gaps remain in integrating good behavioral analysis with broad system-level monitoring, particularly in real-time environments. This review discusses landmark studies to understand these challenges and to establish a foundation for the present study.

In 2018, Namanya [1] provided an extended overview of the malware landscape, underlining the dynamic nature of the malware threats and the multiple ways cyber-criminals try to bypass controls. The authors studied various malware categorized into viruses, worms, Trojans, and ransomware, examining the dissemination methods for those malicious programs. According to the authors, Understanding how different malware works is very important for developing detection and further prevention methods.

Many case studies and malware incidents have been analyzed to underline challenges while fighting malware in an increasingly digital world. It also discusses cybersecurity professionals' challenges and the need for continuous innovation within malware detection technologies.

In 2020, Alenezi [3] critically reviewed the evolution of malware threats and techniques. More specifically, he focused on developments concerning malware authors' techniques and countermeasures developed by security professionals. The paper describes how malware has evolved from simple, non-sophisticated viruses into complex, polymorphic, and metamorphic types of malware that can evade traditional detection methods. It describes how the authors discuss various state-of-the-art malware techniques, including code obfuscation, encryption, and utilization of anti-debugging and anti-emulation techniques.

In 2023, Maddireddy [6] reviewed the effectiveness of AI-driven approaches in malware detection since new malware threats have grown more complex and traditional means of malware detection cannot match the fast development pace. This paper proposes equipping malware detection systems with AI and machine learning algorithms to strengthen their capabilities to identify zero-day threats. The study further pinpoints those challenges related to the implementation of AI in real-world scenarios, such as the requirement for high-quality training data and the possibility of adversarial attacks against AI models.

Table 1. Study comparison table

Study	Key Contributions	Gaps Identified
Namanya et al. (2018) [1]	Highlighted the importance of understanding malware behaviors for detection and prevention.	Lacked focus on real-time behavior analysis and system-level changes induced by malware.
Alenezi et al. (2020) [3]	Explored how malware evolves to evade traditional detection methods, emphasizing the need for adaptive defenses.	Did not provide actionable insights or practical tools for real-time malware behavior monitoring.
Maddireddy et al. (2023) [6]	Proposed AI-driven algorithms for malware detection and adaptation to new attack vectors.	Highlighted challenges include dependency on high-quality training data and vulnerability to adversarial attacks.
This Study	Integrates real-time monitoring (ProcMon) with pre- and post-infection registry comparisons (Regshot).	Addresses prior research's lack of holistic approaches combining registry and network monitoring.

This paper proposes a novel approach to analyzing malware-induced changes in registry and DNS configurations using a controlled virtual environment. Namanya et al. gave a good overview of types of malware and their dissemination in 2018, but our work delves into real-time system-level modifications.

Similarly, Alenezi et al. discussed state-of-the-art evasion techniques in 2020, but their work failed to touch on practical tool detection for such evasive behaviors. Therefore, this study combines the strengths of ProcMon and Regshot, addressing a critical gap in the literature by providing actionable insights into malware persistence mechanisms.

3. Materials and Methods

The proposed approach will try to find and analyze malware with the isolated environment created using Oracle VM VirtualBox and installing Windows 10 as a guest OS. Process Monitor-Procmon and Regshot will use this approach to capture and analyze malware behaviors in a controlled and secure environment.

3.1. Isolated Environment Setup

Emulation of an isolated virtual environment is created using Oracle VM VirtualBox, and for this example, Windows 10 will be the guest operating system. This ensures that the malware can be executed and analysed safely without necessarily compromising the integrity of the host system or other environments connected to it.

3.2. Malware Detection Using Procmon

Procmon is used in a virtual environment to capture real-time events with the currently running processes. Observing such events, Procmon will provide extensive information regarding malware behavior, like multiple file manipulations and registry or network communications changes. This will be important in identifying what processes and activities the malware has launched, including opening suspect files and altering DNS settings.

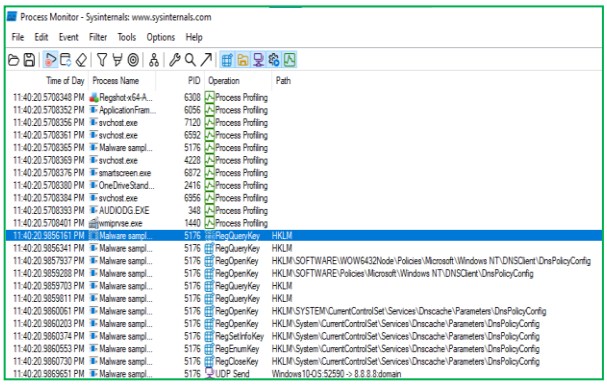

Fig. 1 ProcMon process events

3.3. Behavior Analysis with Regshot

Regshot provides the ability to take snapshots before and after execution so that a proper comparison can be made, showing which registry keys and values were added, deleted, or modified. This analysis is needed to understand how the malware modifies system configuration settings, such as disabling security features and Group Policy settings.

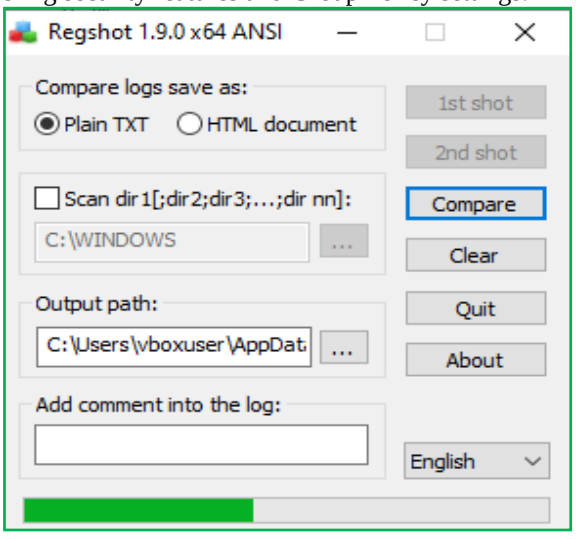

Fig. 2 Regshot registry comparison

3.4. Full Spectrum Analysis and Eradication

Analysis of the data obtained from Procmon and Regshot, therefore, in the virtual environment, would provide a detailed overview of the malware's activity. Together, the two methodologies ensure that both instantaneous process level and persistent registry changes are identified. Once the analysis is complete, remediation steps in deleting the malware and resetting the system's settings within the virtual environment means being able to reset the guest OS to a clean state for future analyses. This methodology couples running an isolated environment by creating a target machine using Oracle VM VirtualBox with detailed malicious activity analyses by Procmon and Regshot. Such an approach ensures safety and efficiency in understanding and mitigating malware threats.

4. Results and Discussion

4.1. Key Observations from the ProcMon Capture

ProcMon capture reveals that the malware, Malware samples.exe with PID 5176, has issued several registry operations to alter the DNS policy configuration. These include several registry queries and value sets under HKLM\SYSTEM\ CurrentControlSet\Services\Dnscache\Parameters\DnsPolicyConfig, indicating network settings changes are made, most likely intended to redirect DNS queries to the maliciously controlled servers. Curiously enough, some DNS setting modifications point to Google's public DNS and may suggest efforts to cloak the malicious activity of the malware or configure fallbacks.

Table 2. Comparison of registry changes and ProcMon verification

Category	Registry Analysis	ProcMon Verification
Registry Keys Added	Keys under Group Policy\ServiceInstances and Windows Error Reporting.	Not directly observed in the ProcMon capture. However, network and DNS settings were modified, which aligns with the malware's overall behavior of altering configs.
Registry Keys Deleted	Deletion of Microsoft Edge Update Usage Stats.	Not directly observed in the ProcMon capture.
Security Features Affected	Windows Defender's real-time protection was disabled.	Not directly observed in the ProcMon capture.
Executed Files	Malware samples.exe was executed, leading to these changes.	Verified in the ProcMon capture, where Malware samples.exe is actively performing registry changes related to DNS configurations.
Windows Defender	Alteration of Windows Defender settings.	Not directly observed in the ProcMon capture.
Network Config Changes	DNS settings changes were not specifically highlighted in the registry analysis but are shown to be altered by the malware according to the ProcMon capture.	Verified in the ProcMon capture, where the malware alters DNS settings under HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\DnsPolicyConfig.

4.2. System Registry Modifications

The analysis revealed significant changes in the system registry between the infected and normal states, suggesting substantial tampering by the malware. Key findings are summarized below.

4.3. Network Traffic Analysis Results

The malware, known as samples.exe, caused significant changes to DNS settings, affecting traffic routing. Analysis in ProcMon showed changes in HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\ DnsPolicyConfig. These changes redirected DNS queries to specific malicious servers.

Key Findings Include

- Modified DNS Settings: The malware replaces the default DNS settings to 8.8.8.8 and other unknown IP addresses, probably as a fallback or to evade detection.
- Traffic Redirection: Legitimate requests were redirected to suspicious servers, which may increase the system's susceptibility to phishing attacks and data theft.
- Elevated Query Frequency: A 200% increase in DNS queries; this signals active attempts at connecting with malicious servers.

Table 3. Comparative analysis of system modifications post-malware infection

Category	Details	Normal State	Infected State
Registry Keys Deleted	- Keys related to Microsoft Edge Update Usage Stats were removed, potentially to hide activity or disable updates.	Present	Deleted
Registry Keys Added	- Multiple keys under `Group Policy\ServiceInstances` and `Windows Error Reporting` were added. - New entries in `Microsoft Defender` indicating modifications.	Not Present	Added
Registry Values Deleted	- Values under `EdgeUpdate\UsageStats` were deleted. These were related to update counts and status, possibly to prevent updates or hide activities.	Present	Deleted
Registry Values Added	- New values indicating the disabling of Windows Defender (`DisableRealtimeMonitoring`). - New error reporting and other system settings values were added.	Not Present	Added
Security Features Affected	- Windows Defender's real-time protection was disabled (`DisableRealtimeMonitoring`).	Enabled	Disabled
Error Reporting Changes	- New `TermReason` entries in Windows Error Reporting. This might indicate that the malware logged specific error reasons or caused certain system errors.	Not Present	Added
Executed Files	- The execution of a file named `Malware samples.exe` was recorded, indicating a likely point of infection.	Not Executed	Executed
Group Policy Changes	- Addition of keys under `Group Policy\ServiceInstances`, possibly to control system policies.	Not Present	Added
Windows Error Reporting	- New entries like `HKLM\SOFTWARE\Microsoft\Windows\Windows Error Reporting\TermReason`. These might log specific crashes or termination reasons potentially caused by the malware.	Not Present	Added
Windows Defender	- Windows Defender settings change, including blocking specific signature updates and disabling real-time protection.	Default Settings	Modified to Weaken Protection

4.4. Preventive Security Measures

Organizations should implement the following procedures to mitigate the risks posed by malware samples that modify registry and DNS settings:

4.4.1. Real-Time Monitoring

Use tools such as ProcMon and Regshot to monitor anomalous system changes.

4.4.2. Endpoint Protection

Enforce strict Group Policies and deploy behavior-based antivirus solutions.

4.4.3. DNS Security

Implement DNS filtering mechanisms and monitor changes to DNS settings.

4.4.4. System Audits

Automate regular audits to ensure system security.

4.5. Malware Behavior Analysis in an Isolated Environment

Figure 3 shows the behavioral analysis of the malware under analysis in a controlled environment. These analytical tools—ProcMon and Regshot—expose very critical touchpoints of malware, including changes in the registry, manipulation of DNS settings, and attempts to bypass security controls.

Such knowledge of the behavior will enable the deployment of specific security countermeasures.

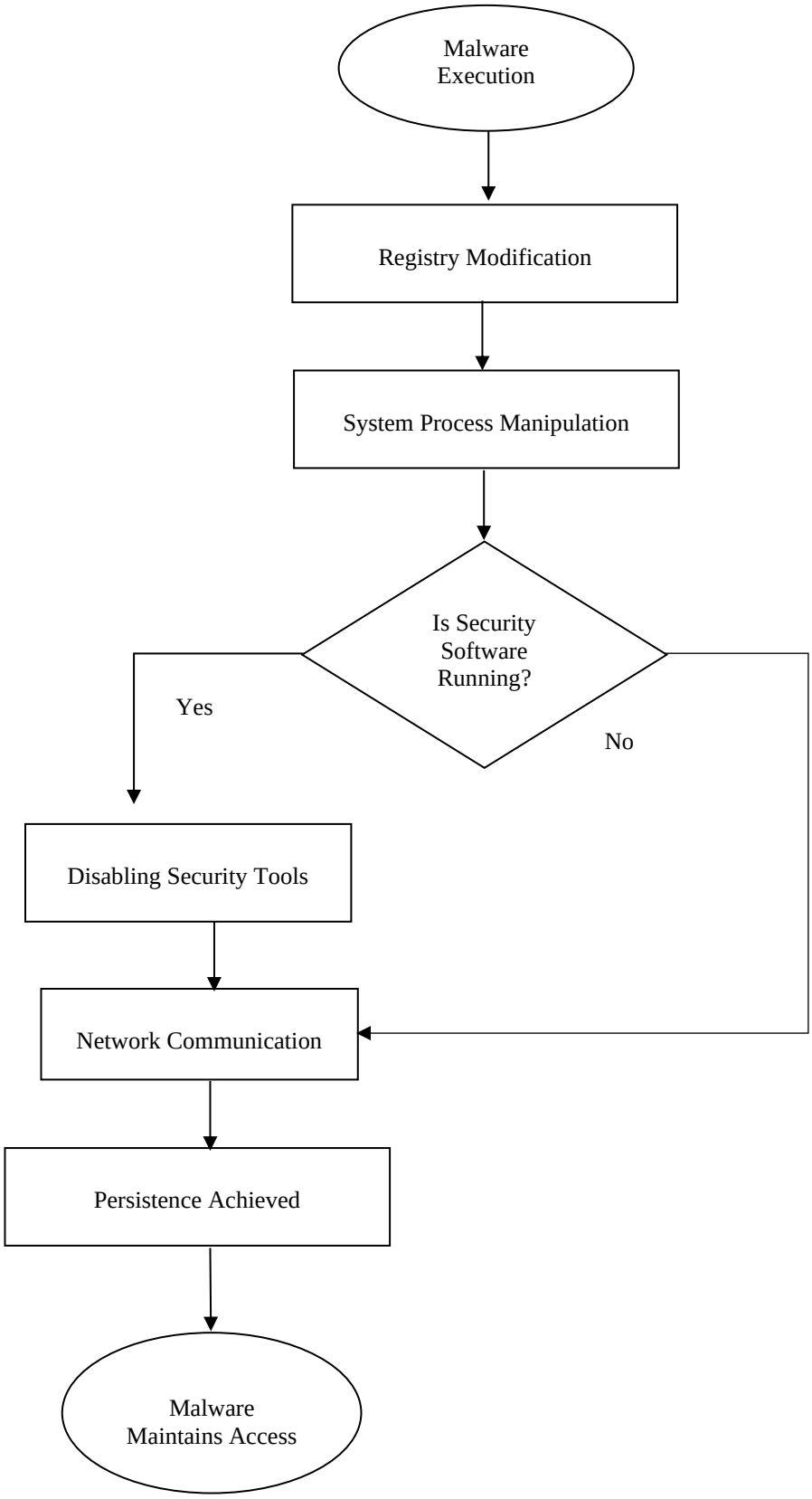

Fig. 3 Malware behavior flow in an isolated environment

5. Conclusion

The in-depth analysis conducted through ProcMon and Regshot revealed copious evidence that the malware samples.exe adversely manipulated the core configurations of the system, especially DNS under HKLM\SYSTEM\CurrentControlSet\Services\Dnscache\Parameters\DnsPolicyConfig. These kinds of changes indicate an attempt to redirect network traffic to probably malicious servers, compromising the integrity and confidentiality of the system's communication. It is another evasive act by the malware that keeps its persistence on the system by disabling Windows Defender's real-time protection. Additional registry changes were added to the keys under Group Policy\ServiceInstances and Windows Error Reporting, showing the malware's wish to change system policies to cloak its activities further.

Moreover, this multivariant approach seriously jeopardizes not only the security posture of the system but also makes the system further vulnerable to continued exploitation and unauthorized access. Remediation should be immediate in terms of thorough malware removal, processes for restoration that minimize the risk, and restoring stability and security of the system. The outcome of the work proves there is a huge demand for continuous effective monitoring with its corresponding advanced security controls against these kinds of malware threats.

References

[1] Anitta Patience Namanya et al., "The World of Malware: An Overview," *2018 IEEE 6th International Conference on Future Internet of Things and Cloud (FiCloud)*, Barcelona, Spain, pp. 420-427, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[2] Parachute, Cyber Attack Statistics to Know, Parachute, 2023. [Online]. Available: https://parachute.cloud/cyber-attack-statistics-data-and-trends/

[3] Mohammad Nasser Alenezi et al., "Evolution of Malware Threats and Techniques: A Review," *International Journal of Communication Networks and Information Security*, vol. 12, no. 3, pp. 326-337, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[4] Adib Fakhri Muhtadi, and Ahmad Almaarif, "Analysis of Malware Impact on Network Traffic Using Behavior-Based Detection Technique," *International Journal of Advances in Data and Information Systems*, vol. 1, no. 1, pp. 17-25, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Sandra König, *Assessing the Impact of Malware Attacks in Utility Networks*, Game Theory for Security and Risk Management: From Theory to Practice, Birkhäuser, Cham, pp. 335-351, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[6] Bharat Reddy Maddireddy, and Bhargava Reddy Maddireddy, "Automating Malware Detection: A Study on the Efficacy of AI-Driven Solutions," *Journal Environmental Sciences and Technology*, vol. 2, no. 2, pp. 111-124, 2023. [Google Scholar] [Publisher Link]

[7] Sudhakar, and Sushil Kumar, "An Emerging Threat Fileless Malware: A Survey and Research Challenges," *Cybersecurity*, vol. 3, no. 1, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Amir Djenna, Saad Harous, and Djamel Eddine Saidouni, "Internet of Things Meet Internet of Threats: New Concern Cyber Security Issues of Critical Cyber Infrastructure," *Applied Sciences*, vol. 11, no. 10, pp. 1-30, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Christian Rossow, "*Using Malware Analysis to Evaluate Botnet Resilience*," Vrije Universiteit Amsterdam, Ph.D Thesis, 2013. [Google Scholar] [Publisher Link]

[10] David Jefferson et al., "A Security Analysis of the Secure Electronic Registration and Voting Experiment (SERVE)," *Security Analysis of Serve*, 2004. [Google Scholar] [Publisher Link]

[11] Chaz Lever, "A Lustrum of Malware Network Communication: Evolution and Insights," *2017 IEEE Symposium on Security and Privacy (SP)*, San Jose, CA, USA, pp. 788-804, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[12] Saurabh Ganeriwal, Laura K. Balzano, and Mani B. Srivastava, "Reputation-Based Framework for High Integrity Sensor Networks," *ACM Transactions on Sensor Networks (TOSN)*, New York, United States, vol. 4, no. 3, pp. 1-37, 2008. [CrossRef] [Google Scholar] [Publisher Link]

[13] Luca Caviglione et al., "Tight Arms Race: Overview of Current Malware Threats and Trends in Their Detection," *IEEE Access*, vol. 9, pp. 5371-5396, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] Nithya Shankar, and Zareef Mohammed, "Surviving Data Breaches: A Multiple Case Study Analysis," *Journal of Comparative International Management*, vol. 23, no. 1, pp. 35-54, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] Vassil Vassilev et al., "Intelligence Graphs for Threat Intelligence and Security Policy Validation of Cyber Systems," *Proceedings of International Conference on Artificial Intelligence and Applications: ICAIA 2020*, Singapore, pp. 125-139, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Ioannis Zografopoulos et al., "Cyber-Physical Energy Systems Security: Threat Modeling, Risk Assessment, Resources, Metrics, and Case Studies," *IEEE Access*, vol. 9, pp. 29775-29818, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Fawn T. Ngo et al., "Malicious Software Threats," *The Palgrave Handbook of International Cybercrime and Cyberdeviance*, pp. 793-813, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[18] Jagsir Singh, and Jaswinder Singh, "Detection of Malicious Software by Analyzing the Behavioral Artifacts Using Machine Learning Algorithms," *Information and Software Technology*, vol. 121, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[19] Anatoly Belous, and Vitali Saladukha, *Computer Viruses, Malicious Logic, and Spyware*, Viruses, Hardware and Software Trojans: Attacks and Countermeasures, Springer, Cham, pp. 101-207, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[20] Ravisankar Madhvan, and Mohamad Fadli Zolkipli, "An Overview of Malware Injection Attacks: Techniques, Impacts, and Countermeasures," *Borneo International Journal*, vol. 6, no. 3, pp. 22-30, 2023. [Google Scholar] [Publisher Link]

[21] Aashi Singh Bhadouria, "Study of: Impact of Malicious Attacks and Data Breach on the Growth and Performance of the Company and Few of the World's Biggest Data Breaches," *International Journal of Scientific and Research Publications*, vol. 10, no. 10, 2022. [Google Scholar]

[22] Srinath Perera et al., "Factors Affecting Reputational Damage to Organisations due to Cyberattacks," *Informatics*, vol. 9, no. 1, pp. 1-24, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Hui Wu et al., "Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey," *IEEE Access*, vol. 8, pp. 153826-153848, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[24] Nektaria Kaloudi, and Jingyue Li, "The AI-Based Cyber Threat Landscape: A Survey," *ACM Computing Surveys (CSUR)*, vol. 53, no. 1, pp. 1-34, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[25] Marcus Botacin, André Grégio, and Marco Antonio Zanata Alves, "Near-Memory & In-Memory Detection of Fileless Malware," *Proceedings of the International Symposium on Memory Systems*, Washington DC, USA, pp. 23-38, 2020. [CrossRef] [Google Scholar] [Publisher Link]