International Journal of P2P Network Trends and Technology
ISSN: 2249–2615 / https://doi.org/10.14445/22492615/IJPTT-V16I1P401
Volume 16 Issue 1, 1-7, Jan-April 2026

Original Article

A Critical Analysis of Different Malware Analysis Techniques and How They Can Be Incorporated into the Process of Cyber Kill Chain to Enhance the Overall Effectiveness

Kultar Singh

Institut für Cybersicherheit, Fachhochschule des Mittelstands (FHM) - Campus Düren, Deutschland und University of Gloucestershire, United Kingdom.

Corresponding Author : Kultarsingh355@gmail.com

Received: 06 February 2026 Revised: 12 March 2026 Accepted: 29 March 2026 Published: 13 April 2026

Abstract - *In order to improve overall cybersecurity efficacy, this research study seeks to critically assess a variety of malware analysis methodologies and investigate how they might be integrated into the Cyber Kill Chain framework. This study examines both established and novel techniques for analyzing malware, evaluates their advantages and disadvantages, and suggests tactical points of integration for the Cyber Kill Chain. Organizations can strengthen their defenses against complex cyberattacks by combining these components.*

Keywords - *Cyber Security, Cyber Kill Chain, Analyzing Malware, Organization, Cyber Attack.*

1. Introduction

1.1. Background

The ongoing increase in cyberthreats presents serious difficulties for businesses throughout the globe in the dynamic field of cybersecurity. Security experts must take preventative action since malevolent actors are always improving their tactics. Originally presented by Lockheed Martin, the Cyber Kill Chain architecture has grown to be a key component in comprehending and reducing cyberthreats (Aidoo, 2019). This framework offers a methodical approach to defense by outlining the phases of a cyberattack. This research is being done against the backdrop of malware becoming more sophisticated and the requirement for a comprehensive defensive plan. Malware comes in many forms, from conventional viruses to Advanced Persistent Threats (APTs), and each one has unique traits that call for careful examination. A critical review of current malware analysis methods is essential as well-funded and highly competent attackers target enterprises more and more(Humayun et al., 2020).

1.2. Purpose of the Study

The study's main goal is to critically and thoroughly analyze different malware analysis methods, with an emphasis on how well they integrate into the Cyber Kill Chain framework. Our goal in analyzing the pros and cons of various malware analysis techniques is to pinpoint critical places of integration inside the Cyber Kill Chain(Humayun et al., 2020). By strengthening each link in the Cyber Kill Chain, this integration aims to improve an organization's cybersecurity posture as a whole. The goal of this research is to close the gap that exists between theoretical frameworks and actual applications. The Cyber Kill Chain offers a theoretical road map for comprehending cyber threats, but for practical use, malware analysis methods must be successfully implemented inside this framework. Thus, the goal of this study is to provide practitioners in cybersecurity with easily implementable insights and recommendations (Aidoo, 2019).

1.3. Scope and Limitations

The study's scope includes a thorough investigation of both established and novel malware analysis methods. It explores sandboxing, machine learning techniques, behavioral analysis, heuristic analysis, and signature-based detection. All seven phases of the Cyber Kill Chain's integration will be examined, offering a comprehensive understanding of how each method might aid in threat prevention(Aidoo, 2019). It is imperative to recognize the inherent limits of this research. Due to the fast-changing nature of cyber threats, the situation may change while the study is being conducted. Furthermore, different threat scenarios, organizational context, and resource availability may all have an impact on how effective integrated

techniques are. Notwithstanding these drawbacks, the goal of this research is to provide an insightful analysis that advances the current discussion on improving cybersecurity resilience(Humayun et al., 2020).

2. Discussion and Analysis

2.1. Technique of Malware Analysis

Malware, which stands for malicious software, is a ubiquitous and always-changing danger to cybersecurity. To combat these threats effectively, one must have a sophisticated understanding of malware analysis methods(Kara, 2019). This section offers a thorough examination of several strategies, each with special advantages and disadvantages, setting the groundwork for their incorporation into the Cyber Kill Chain paradigm(Sibi Chakkaravarthy, Sangeetha, and Vaidehi, 2019).

2.1.1. Static Analysis

Static analysis is the process of analyzing a malware sample's properties without running it. This technique, which is based on established signatures or patterns, is very helpful in swiftly recognizing risks.

Signature-Based Detection

Static analysis's mainstay is signature-based detection, which uses pre-defined malware fingerprints or signatures. By checking file signatures against a database of known dangerous signatures, this technique functions similarly to antivirus software(Sibi Chakkaravarthy, Sangeetha, and Vaidehi, 2019). Even though it works well against known threats, polymorphic or zero-day malware—which continuously modifies its code to avoid being detected by signatures—makes its shortcomings clear(Or-Meir et al., 2019).

Heuristic Analysis

Within static analysis, heuristic analysis adopts a more dynamic approach. Rather than depending on particular signatures, it recognizes trends and actions suggestive of malicious software. Heuristics are more adaptive to dangers that have not been observed before because they use rules and algorithms to identify suspicious activity(Or-Meir et al., 2019). On the other hand, it might produce false positives and have trouble with more complex malware that imitates real behavior.

2.1.2. Dynamic Analysis

In dynamic analysis, a malware sample is run in a lab setting so that its behavior may be tracked in real time(Kara, 2019). This method offers insights into the malware's behavior, enabling a more comprehensive comprehension of its features.

Behavioral Analysis: The main goal of behavioral analysis is to see how a malware specimen behaves and interacts while it is being executed. Analysts can spot malicious activity that static analysis would miss by keeping an eye on system behavior and network connections(Kara, 2019). Because this technique does not rely on predetermined signatures, it works especially well against attacks that are polymorphic or zero-day. It might, however, have trouble telling the difference between harmful and benign activity, necessitating more context to make an appropriate assessment(McDole et al., 2020).

Sandboxing: Through the use of sandboxing, separate environments are created in which malware samples can be run without endangering the host system(McDole et al., 2020). Analysts may watch a malware's whole lifecycle in this regulated environment, from its first execution to any possible lateral movement within a network. By capturing the dynamic nature of emerging threats, sandboxing improves the detection of them. However, clever malware can sense the virtual environment and change its behavior to avoid detection(Kara, 2019).

2.1.3. Hybrid Analysis

Hybrid analysis aims to integrate static and dynamic analysis methods, acknowledging their respective advantages and disadvantages, to provide a more thorough comprehension of malware.

Combining Static and Dynamic Approaches

Hybrid analysis overcomes the shortcomings of each analysis method by utilizing the advantages of both static and dynamic analysis. In order to swiftly identify known threats using heuristic analysis and signature-based detection, static analysis is first performed (McDole et al., 2020). The discovered samples are next subjected to dynamic analysis in a controlled environment in order to reveal their behavioral characteristics. This combination raises the overall efficiency of the analytical process and increases the accuracy of threat detection (Dutta et al., 2021).

2.1.4. Machine Learning in Malware Analysis

Using algorithms to find patterns and abnormalities in massive datasets, Machine Learning (ML) has become a potent tool in the field of malware analysis.

Anomaly Detection

The goal of machine learning-based anomaly detection is to find instances where a system deviates from expected behavior. It is possible to identify abnormalities suggestive of malicious activity by training models on typical network and system operations(Or-Meir et al., 2019). While anomaly detection is very useful for spotting new threats, it can also lead to false positives in situations that are dynamic and complicated(McDole et al., 2020).

Pattern Recognition

Because machine learning algorithms are so good at recognizing patterns, it is possible to find similarities between different malware samples(Or-Meir et al., 2019). The ability to identify patterns improves the classification and categorization of malware, offering information about

possible connections between various threats. However, the caliber and variety of the training data have a major impact on how well machine learning models perform(Sibi Chakkaravarthy, Sangeetha, and Vaidehi, 2019).

Strengthening cybersecurity defenses requires a thorough understanding of malware analysis techniques. While dynamic analysis—which includes behavioral analysis and sandboxing—offers deeper insights into the behavior of sophisticated malware, static analysis gives speedy identification of recognized threats(Kara, 2019).

2.2. Cyber Kill Chain

2.2.1. Overview

Lockheed Martin devised a concept called the Cyber Kill Chain, which is a strategic framework for comprehending the lifecycle of a cyberattack. The implementation of segmenting the assault process into discrete stages enables businesses to proactively identify and neutralize risks(Dargahi et al., 2019). Through a thorough comprehension of every stage, from preliminary reconnaissance to accomplishing the enemy's goals, defenders can formulate focused countermeasures and defenses. An outline of the Cyber Kill Chain is given in this section, which prepares the reader for the critical examination and incorporation of malware analysis methods(Nikkhah Bahrami et al., 2019).

2.2.2. Stages of the Cyber Kill Chain

Reconnaissance

The information-gathering phase, known as reconnaissance, is the initial stage. The goal of adversaries is to locate weak places, possible points of entry, and valuable resources in the target environment. Passive data collection techniques, including looking up information on the internet or keeping an eye on social media, are frequently used to describe this phase (Nikkhah Bahrami et al., 2019). Utilizing threat intelligence feeds to identify known threat actors and their Tactics, Methods, and Procedures (TTPs) can be one way to integrate malware analysis methodologies at this point. Indicators of Compromise (IOCs) may be found in publicly available datasets by proactive reconnaissance using static analysis, improving the organization's capacity to foresee and counter possible attacks(Dargahi et al., 2019).

Weaponization

Adversaries create the exploit payloads or malicious tools that will be employed in the attack during the weaponization stage. In order to exploit vulnerabilities found during reconnaissance, this may entail developing original malware or reusing already-existing ones(Ahmed, Asyhari, and Arafatur Rahman, 2021). Here, static analysis—looking for recognized signatures or patterns in the code of possible weaponized payloads—must be the primary focus when integrating malware research tools. Additionally, suspicious code structures or behaviors suggestive of weaponized malware might be found via heuristic analysis. Defenders can proactively implement countermeasures, like updated antivirus signatures or intrusion detection signatures, by having a thorough understanding of the weaponization process(Hoffmann, 2019).

Delivery

The weaponized payload is introduced into the target environment at the time of delivery. Numerous things, such as hacked third-party software, malicious websites, or email attachments, might cause this(Hoffmann, 2019). At this point, dynamic analysis—especially sandboxing—becomes essential. Analysts can watch how the possibly harmful code behaves and spot any malicious activity by running it in a controlled environment. Novel risks that could have eluded traditional static analysis can be quickly identified thanks to our real-time analysis (Ahmed, Asyhari, and Arafatur Rahman, 2021).

Exploitation

Adversaries use vulnerabilities to obtain unauthorized access to the target system during the exploitation stage. Here, behavioral analysis is crucial because it enables defenders to keep an eye out for and recognize any unexpected or malicious activity connected to the exploitation process (Ahmed, Asyhari, and Arafatur Rahman, 2021). Organizations can block an assault before it escalates by deploying response mechanisms and targeted protections based on their understanding of the behaviors that indicate exploitation efforts.

Installation

After an adversary's exploitation is successful, they proceed to the Installation phase, where they create a long-term presence within the compromised system(Dargahi et al., 2019). At this point, hybrid analysis—which combines static and dynamic approaches—works well. While dynamic analysis shows the strategies and methods used by the deployed malware, static analysis aids in the identification of known malicious artifacts. By using an integrated method, defenders may create thorough remediation plans and stop additional compromise(Nikkhah Bahrami et al., 2019).

Command and Control

Establishing communication channels between the compromised system and the infrastructure that is under the control of an external attacker is the task of the Command and Control (C2) stage(Ahmed, Asyhari, and Arafatur Rahman, 2021). In this case, machine learning anomaly detection is very important because it can recognize odd network traffic patterns or behaviors that point to hostile C2 activity. Defenders can prevent the attacker from controlling the compromised systems by proactively identifying and thwarting these communications(Dargahi et al., 2019).

Actions on Objectives

The adversary's efforts to accomplish their ultimate aims within the target environment culminate in the last stage,

Actions on Objectives. This might entail manipulating systems, stealing data, or using other nefarious measures(Nikkhah Bahrami et al., 2019). At this point, post-infection analysis—a hybrid analysis component—becomes crucial. Defenders can improve their defenses, learn more about the adversary's goals, and create countermeasures to stop similar attacks in the future by studying the attack's aftermath(Dutta et al., 2021).

2.3. Integration points within the Cyber Kill Chain

2.3.1. Reconnaissance

The Cyber Kill Chain's initial stage, reconnaissance, is when malware analysis techniques are first integrated. A key component of proactive threat intelligence is the methodical gathering and examination of data regarding possible threats prior to their materialization(Straub, 2020). At this point, possible attackers and their strategies can be identified with the help of static analysis tools, such as looking through past threat data and known Indications of Compromise (IOCs). Organizations can proactively identify malevolent individuals, comprehend their objectives, and strengthen their defenses against potential attacks by utilizing threat intelligence feeds and databases(HosseiniNejad et al., 2019).

2.3.2. Weaponization

Signature-Based Detection

When the Cyber Kill Chain reaches the weaponization phase, it is critical to incorporate signature-based detection. This method, which makes use of static analysis, compares the traits of weaponized payloads to known malware signatures(Straub, 2020). Security systems that incorporate updated signature databases allow enterprises to quickly detect and stop harmful payloads that correspond to known patterns. Although it works well against recognized threats, it might not be able to identify new or polymorphic malware, which calls for the use of supplementary methods(Mirza et al., 2021).

Behavioral Analysis

In the Weaponization stage, behavioral analysis plays a critical role in enhancing signature-based detection. Using a controlled environment, this dynamic analysis technique looks at potentially dangerous code's behavior(HosseiniNejad et al., 2019). Through real-time analysis of the weaponized payload's movements, analysts are able to spot departures from typical behavior. By improving the identification of threats that are polymorphic and zero-day, which can elude standard signature-based methods, behavioral analysis offers a stronger line of defense against highly skilled adversaries(Mirza et al., 2021).

2.3.3. Delivery

Sandboxing and Dynamic Analysis

The point at which malware becomes a weapon and enters the target environment is known as delivery. A dynamic analytic approach called sandboxing establishes separate settings in which possible dangers can be seen and investigated without endangering the host system. Sandboxing is especially useful for revealing how malware behaves when it is being executed, which helps identify dangerous activity that static analysis could miss. The organization's capacity to identify and comprehend the nature of incoming threats before they escalate is improved by integrating sandboxing at this point(Haga, Meland, and Sindre, 2020).

Machine Learning for Payload Detection

During the Delivery stage, Machine Learning (ML) plays a crucial role in improving payload detection. ML algorithms that have been trained on a variety of datasets can identify trends and abnormalities that point to malicious payloads(Mirza et al., 2021). Machine learning algorithms are capable of adapting to identify new and complex threats by utilizing past data and learning from dynamic threat landscapes. A proactive layer of defense is added by incorporating machine learning into payload detection methods, which strengthens the organization's resistance to new threats and complements conventional analytic techniques(HosseiniNejad et al., 2019).

2.3.4. Exploitation

In the Cyber Kill Chain's Exploitation phase, behavioral analysis takes center stage. As adversaries leverage vulnerabilities to obtain unauthorized access, it becomes imperative to monitor the system's activities(HosseiniNejad et al., 2019). Unusual behavior linked to exploitation efforts, including privilege escalation or lateral network migration, can be found using behavioral analysis. By incorporating behavioral analysis at this point, defenders can minimize possible harm and stop additional compromise by quickly identifying and countering exploitation(Straub, 2020).

2.3.5. Installation

Signature-Based Detection

After the hack has been successfully exploited, the Installation step entails creating a lasting presence within the compromised system(Straub, 2020). At this point, companies can identify and stop known malware artifacts connected to the installation process by integrating signature-based detection. Defenders can quickly react to and neutralize known threats by using up-to-date signature databases, which keep them from getting a foothold in the environment(Mirza et al., 2021).

Hybrid Analysis

Taking into account the intricacy of the Installation phase, hybrid analytic integration becomes essential. Hybrid analysis, which combines static and dynamic techniques, enables analysts to recognize implanted malware's strategies in addition to recognized artifacts. By using a comprehensive approach, the company may better build customized remediation procedures that address all potential dangers within the affected system(Haga, Meland, and Sindre, 2020).

2.3.6. Command and Control

Establishing communication connections between the compromised system and external infrastructure controlled by the attackers is the task of the Command and Control (C2) stage. The machine learning-based technique known as anomaly detection plays a crucial role in spotting odd network traffic patterns or behavior that point to hostile C2 activity(Mirza et al., 2021). Organizations can hinder the adversary's ability to operate the compromised systems by proactively detecting and blocking malicious communications by integrating anomaly detection at this point(Haga, Meland, and Sindre, 2020).

2.3.7. Actions on Objectives

Actions on Objectives, the last phase of the Cyber Kill Chain, demands a post-infection analysis and remediation strategy. Identifying the goals of the enemy, creating plans to stop future attacks, and carefully examining the attack's aftermath are all necessary to integrate this stage(Straub, 2020). This stage typically involves reviewing logs, performing forensic analysis, and evaluating the attack's effects in retrospect. Organizations may strengthen their cybersecurity posture against upcoming attacks, improve their defenses, and execute focused remediation steps by comprehending the adversary's goals(HosseiniNejad et al., 2019).

2.4. Case Study Analysis

2.4.1. Case Study 1: Stuxnet

The extremely intelligent worm Stuxnet was found in 2010 and is a prime example of a Cyber Kill Chain integration gone wrong(Bahtiyar, Yaman, and Altınığne, 2019). This virus demonstrated the use of behavioral analysis, anomaly detection, and signature-based detection. It was created with the intention of attacking Iran's nuclear facilities.

Reconnaissance

In order to learn more about the target facility's systems and weaknesses, Stuxnet's developers conducted a thorough investigation(Stevens, 2019).

Weaponization

The identification of the distinct code signatures linked to Stuxnet was made possible by the use of signature-based detection(Bahtiyar, Yaman, and Altınığne, 2019). This enabled security specialists to comprehend the malevolent behavior of the worm in conjunction with behavioral analysis.

Delivery

Stuxnet used a number of delivery techniques, such as network vulnerabilities and USB sticks. Understanding the behavior of the malware and stopping its spread were made possible by the use of sandboxing and dynamic analysis(Stevens, 2019).

Exploitation

Unauthorized access and manipulation of Programmable Logic Controllers (PLCs) were among the exploitation efforts made by Stuxnet that were identified largely through behavioral analysis.

Installation

Stuxnet's presence was detected via signature-based detection, and its strategies were revealed through hybrid analysis. This integration made it easier to eradicate the malware from infected systems(Stevens, 2019).

Command and Control

In order to stop Stuxnet from communicating with its command and control servers, anomaly detection played a critical role in spotting odd network patterns.

Actions on Goals

Post-infection study identified the goals of Stuxnet, which aided in the creation of remediation plans and provided guidance for upcoming defenses against comparable threats(Bahtiyar, Yaman, and Altınığne, 2019).

2.4.2. Case Study 2: WannaCry Ransomware

The 2017 WannaCry ransomware assault served as a prime example of the value of integrating malware research tools into early detection and response processes.

Reconnaissance

WannaCry took advantage of a Microsoft Windows vulnerability. This vulnerability may have been found and fixed before the attack with proactive threat intelligence (Akbanov, 2019).

Weaponization

The known malware signatures of WannaCry were successfully recognized by signature-based detection. Its unusual conduct would have been recognized with the use of behavioral analysis, allowing for prompt action(KAO, HSIAO, and TSO, 2019).

Delivery

WannaCry's behavior may have been identified during the delivery phase by dynamic analysis, especially sandboxing, which would have stopped the virus's execution and propagation(Akbanov, 2019).

Exploitation

Unusual actions connected to the ransomware's attempts to take advantage of vulnerabilities would have been discovered using behavioral analysis used for exploit detection(KAO, HSIAO, and TSO, 2019).

Installation

WannaCry would have been located and eliminated from compromised systems through the use of hybrid analysis in conjunction with signature-based detection(Akbanov, 2019).

Command and Control

Unusual network traffic suggestive of WannaCry's communication with its command and control infrastructure may have been detected by anomaly detection and prevented(KAO, HSIAO, and TSO, 2019).

Actions on Goals

By gaining knowledge of the ransomware's intentions, post-infection analysis could have improved repair efforts and fortified defenses going forward (Akbanov, 2019).

2.4.2. Lessons learned from Past Incidents

Key to Adaptability

Cyber threats are dynamic, thus a protection plan that adapts to them is necessary. By combining several malware analysis methods, companies can react to new or unknown threats in an efficient manner(Chuquilla, 2019).

Cooperation and Information Sharing

Within the cybersecurity sector, Stuxnet brought to light the significance of cooperative efforts and information sharing(Aljaidi, 2022). Shared information and proactive threat intelligence can strengthen group defenses and get organizations ready for future attacks.

Multifaceted Defense

The necessity for a multiple security strategy was highlighted by ransomware assaults such as WannaCry. Even while signature-based detection is essential, the overall security posture is strengthened when behavioral analysis, sandboxing, and anomaly detection are added(Chuquilla, 2019).

Continuous Improvement and Patching

Finding vulnerabilities is a common task during the reconnaissance phase. Proactive defensive tactics must include regular patching, ongoing enhancement, and remaining up to date on new threats(Aljaidi, 2022).

Post-Infection Analysis

Examining historical events offers insightful information for upcoming defenses(Chuquilla, 2019). Post-infection analysis assists businesses in strengthening their defenses against comparable threats, improving their detection techniques, and comprehending the strategies used by the enemy.

3. Recommendation

3.1. Invest in Proactive Threat Intelligence

To foresee and get ready for possible threats during the reconnaissance stage, organizations should give top priority to the collection and analysis of threat intelligence(Zengy, 2022).

3.2. Establish a Multilayered Security

By combining behavioral analysis, dynamic analysis, and signature-based detection with sandboxing, you may create a security strategy that effectively combats both known and unknown threats(McDonnell, 2021).

3.3. Integrate Machine Learning for Proactive Defense

By putting machine learning algorithms for pattern recognition and anomaly detection into practice, defense mechanisms gain a proactive layer that makes it possible to identify new threats(Zengy, 2022).

3.4. Encourage Cooperation and Information Sharing

To bolster group cybersecurity defenses, organizations should actively participate in cooperative efforts to share threat intelligence and lessons gained(McDonnell, 2021).

3.5. Perform Regular Post-Infection Analysis

A comprehensive grasp of previous events is necessary for ongoing progress. Frequent post-infection analysis helps businesses change and adapt to new threat landscapes by providing information for future defenses(Zengy, 2022).

4. Conclusion

The study is a comprehensive description of how to improve Cyber Kill Chain efficacy through the integration and critical analysis of malware analysis methodologies. A strong defense against developing cyber threats is provided by the strategic integration of proactive threat intelligence, signature-based detection, behavioral analysis, sandboxing, machine learning, and hybrid analysis within the Cyber Kill Chain. Each stage benefits from customized malware analysis techniques, from the reconnaissance phase—where threat intelligence drives proactive defenses—to the actions-on-objectives phase, when post-infection analysis informs remediation tactics. Case studies from the real world, like WannaCry and Stuxnet, highlight how well this integrated strategy works to resist highly skilled cyber adversaries.

References

[1] Yussuf Ahmed, A. Taufiq Asyhari, and Md. Arafatur Rahman, "Cyber Kill Chain Approach for Detecting Advanced Persistent Threats," C*omputers, Materials & Continua*, vol. 67, no. 4, pp. 2497-2513, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Francis Kwesi Aidoo, "End Users Security Awareness Campaign from Information Security Threats, Vulnerabilities and Concurrent Cyber-Attacks," *Texila International Journal of Academic Research*, vol. 4 no. 2, pp. 195-201, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[3] M. Akbanov, V.G. Vassilakis, and M.D. Logothetis, "WannaCry Ransomware: Analysis of Infection, Persistence, Recovery Prevention and Propagation Mechanisms," *Journal of Telecommunications and Information Technology*, 2019. [Google Scholar]

[4] Mohammad Aljaidi et al., "NHS WannaCry Ransomware Attack: Technical Explanation of The Vulnerability, Exploitation, and Countermeasures," *International Engineering Conference on Electrical, Energy, and Artificial Intelligence*, pp. 1-6, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[5] Şerif Bahtiyar, Mehmet Barış Yaman, and Can Yılmaz Altınığne, "A Multi-Dimensional Machine Learning Approach to Predict Advanced Malware," *Computer Networks*, vol. 160, pp. 118-129, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[6] Alejandro Chuquilla, Teresa Guarda, and Geovanni Ninahualpa Quiña, "Ransomware - WannaCry Security is Everyone's," *14th Iberian Conference on Information Systems and Technologies*, pp. 1-4, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[7] Tooska Dargahi et al., "A Cyber-Kill-Chain Based Taxonomy of Crypto-Ransomware Features," *Journal of Computer Virology and Hacking Techniques*, vol. 15 no. 4, pp. 277-305, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[8] Nitul Dutta et al., "Introduction to Malware Analysis," *Cyber Security: Issues and Current Trends*, pp. 129-141, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Kristian Haga, Per Håkon Meland, and Guttorm Sindre, "Breaking the Cyber Kill Chain by Modelling Resource Costs," *Graphical Models for Security*, pp. 111-126, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[10] Romuald Hoffmann, "Markov Models of Cyber Kill Chains with Iterations," *International Conference on Military Communications and Information Systems*, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[11] Reyhaneh Hosseini Nejad et al., "A Cyber Kill Chain Based Analysis of Remote Access Trojans," *Handbook of Big Data and IoT Security*, pp. 273-299, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] Mamoona Humayun et al., "Cyber Security Threats and Vulnerabilities: A Systematic Mapping Study," *Arabian Journal for Science and Engineering*, vol. 45, no. 1, pp. 3171-3189, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[13] Da-Yu Kao, Shou-Ching Hsiao, and Raylin Tso, "Analyzing WannaCry Ransomware Considering the Weapons and Exploits," *21st International Conference on Advanced Communication Technology*, pp. 1098-1107, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[14] Ilker Kara, "A Basic Malware Analysis Method," *Computer Fraud & Security*, vol. 2019 no. 6, pp. 11-19, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[15] Andrew McDole et al., "Deep Learning Techniques for Behavioral Malware Analysis in Cloud IaaS," *Malware Analysis Using Artificial Intelligence and Deep Learning*, pp. 269-285, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[16] Serena McDonnell et al., "*CyberBERT: A Deep Dynamic-State Session-Based Recommender System for Cyber Threat Recognition*," *IEEE Aerospace Conference*, pp. 1-12, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[17] Qublai K. Ali Mirza et al., "*Ransomware Analysis using Cyber Kill Chain*," *8th International Conference on Future Internet of Things and Cloud*, pp. 58-65, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Pooneh Nikkhah Bahrami et al., "Cyber Kill Chain-Based Taxonomy of Advanced Persistent Threat Actors: Analogy of Tactics, Techniques, and Procedures," *Journal of Information Processing Systems*, vol. 15, no. 4, pp. 865-889, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ori Or-Meir et al., "Dynamic Malware Analysis in the Modern Era—A State of the Art Survey," *ACM Computing Surveys*, vol. 52, no. 5, pp. 1-48, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[20] S. Sibi Chakkaravarthy, D. Sangeetha, and V. Vaidehi, "A Survey on Malware Analysis and Mitigation Techniques," *Computer Science Review*, vol. 32, pp. 1-23, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[21] Clare Stevens, "Assembling Cybersecurity: The Politics and Materiality of Technical Malware Reports and the Case of Stuxnet," *Contemporary Security Policy*, vol. 41, no. 1, pp. 129-152, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[22] Jeremy Straub, "Modeling Attack, Defense and Threat Trees and the Cyber Kill Chain, ATT amp;CK and STRIDE Frameworks as Blackboard Architecture Networks," *IEEE International Conference on Smart Cloud (SmartCloud)*, pp. 148-153, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[23] Jun Zengy et al., "SHADEWATCHER: Recommendation-guided Cyber Threat Analysis using System Audit Records," *IEEE Symposium on Security and Privacy*, pp. 489-506, 2022. [CrossRef] [Google Scholar] [Publisher Link]