A close-up of a coat of arms

Description automatically generated

University of Gloucestershire

School of Computing and Engineering

MSc in Cyber Security

2023/2024

**ENHANCING CYBERSECURITY: A CRITICAL ANALYSIS OF MALWARE ANALYSIS TECHNIQUES AND THEIR INTEGRATION INTO THE CYBER KILL CHAIN**

Author: Faraz Saeed Khwaja (s4319980)

**Table of Contents**

[Introduction 2](#_Toc177583442)

[Literature Review 3](#_Toc177583443)

[Overview of Malware Analysis Techniques 4](#_Toc177583444)

[Review of Existing Literature on Malware Analysis and Cyber Kill chain 4](#_Toc177583445)

[Identification of Key Concepts and Gaps 5](#_Toc177583446)

[Conclusion of Literature Review 6](#_Toc177583447)

[Malware Analysis Techniques 6](#_Toc177583448)

[Static Analysis 7](#_Toc177583449)

[Dynamic Analysis 7](#_Toc177583450)

[Hybrid Analysis 8](#_Toc177583451)

[Malware Analysis Techniques Comparison 8](#_Toc177583452)

[Machine Learning and Artificial Intelligence in Malware Analysis 9](#_Toc177583453)

[Relevance to the Cyber Kill Chain 10](#_Toc177583454)

[Integration of Malware Analysis Techniques into the Cyber Kill Chain 10](#_Toc177583455)

[Reconnaissance Stage 11](#_Toc177583456)

[Weaponization Stage 11](#_Toc177583457)

[Delivery Stage 12](#_Toc177583458)

[Exploitation Stage 12](#_Toc177583459)

[Installation Stage 13](#_Toc177583460)

[Command and Control (C2) Stage 13](#_Toc177583461)

[Actions on Objectives Stage 13](#_Toc177583462)

[Malware Analysis Techniques into Cyber Kill Chain Stages 14](#_Toc177583463)

[Challenges and Opportunities 15](#_Toc177583464)

[Conclusion 16](#_Toc177583465)

[References 17](#_Toc177583466)

# Introduction

Cybersecurity is essential in fighting increasingly sophisticated malware attacks, which can infiltrate systems, steal data, and disrupt operations. The Cyber Kill Chain framework developed by Lockheed Martin in 2011 is a widely recognized model in cybersecurity that delineates the stages of the cyber-attacks. It comprises seven distinct phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action in objectives. This structure approach allows cybersecurity professionals to analyze and understand the methodologies employed by attackers particularly in the context of advanced persistent threats (APTs) (Liu et al., 2020; Ahmed et al., 2021). With the rise of increasingly malware attacks organization face significant threats to their security. Malware such as, viruses, ransomware and spyware can disrupt operations steal sensitive data and compromise entire network. Understanding the CKC is crucial for organization aiming to enhance their cybersecurity posture. Each phase of the kill chain presents opportunities for defenders to disrupt the attacks process. For instance, effective countermeasure during the reconnaissance phase can significantly hinder an attacker’s ability to gather information about the target thereby reducing the likelihood of the successful exploitation (Huang, 2024; Rashid, 2023).

The objective of this research is to critically assess how various malware analysis techniques (static, dynamic, hybrid analysis and machine learning) can be integrated into the cyber kill chain framework to enhance detection, response, and mitigation strategies against changing cyber threats. This study seeks to explore the most effective ways these techniques can be applied at each stage of the cyber kill chain evaluating their strengths and limitation in enhancing threat detection and response capabilities. Additionally, the research will identify the challenges and opportunities associated with integrating theses malware analysis methods within modern cybersecurity framework like the CKC with a particular focus on improving early detection, mitigation, and system resilience.

# Literature Review

Due to the constant changes in the type of threats present in the cyber world, there is need to invent and enhance the methods of identifying, combating, and eradicating the threat of malware. Many papers have been published in the past to compare the methods and the role of malware analysis in tacticians such as the Cyber Kill Chain. This paper aims at surveying the existing literature on malware analysis techniques and the Cyber Kill Chain to understand the concepts, the advantages, and the limitations of the current research.

## Overview of Malware Analysis Techniques

Malware analysis techniques are essential for understanding and mitigation the threats posed by malicious software. These techniques can be broadly categorized into static, dynamic and hybrid analysis. Static analysis involves examine the malwares code without executing it, allowing researchers to identify signatures and patterns indicative of malicious behavior. However, this method is often hindered by obfuscation techniques employed by malware authors such as binary packing and encryption (Rieck et al., 2011). Dynamic analysis on the other hand executing the malware in a controlled environment (sandbox) to observe its behavior in real time which provides insights into its operational tactics and interactions with the system (Kawakoya et al., 2019; Bayer et al., 2010). This approach is particularly effective for detecting evasive malware that may evade static detection methods. Hybrid analysis combines both static and dynamic techniques leveraging the strengths of each to improve detection accuracy and efficiency (Shosha et al., 2013; Talukder and Talukder, 2020). Recent advanced in machine learning and artificial intelligence have further enhanced malware analysis capabilities by enabling automated detection and classification of malware variants even those that are previously unseen (Liu et al., 2020). Overall, the continuous evolution of malware necessitates the ongoing development and refine of these analysis techniques to effectively combat emerging threats.

## Review of Existing Literature on Malware Analysis and Cyber Kill chain

Malware analysis has emerged as a crucial component in modern cybersecurity with researchers exploring various techniques to understand malicious software. Current research focuses on primary methods of malware analysis: static analysis, dynamic analysis, and hybrid techniques.

Static analysis involves examining the binary code of malware without executing it allowing researchers to identify signatures, structure, and potentially harmful patterns (Shijo et al., 2015). Dynamic analysis involves executing malware in a controlled environment (e.g., a sandbox) to observe its real time behavior. This technique provides insight of the malware runtime behaviors such as file system modification, network, communication, and memory usage (EI Merabet et al., 2019). Hybrid techniques combining both static and dynamic analysis are increasingly seen as the most effective approach for comprehensive malware analysis (Aboaoja et al., 2022).

Malware analysis and cyber kill chain highlights significant progress and ongoing challenges in cybersecurity. Kumar et al (2020) highlight the important of various malware analysis techniques for understanding malicious behavior, which helps in optimizing detection methods. Moneva (2023) connects psychological paradigms to the CKC enhancing the understanding of cybercriminal decision making. Additionally, Kong (2023) discusses the limitation of conventional defense mechanisms against advanced threats presented by CKC advocating for more proactive strategies.

The cyber kill chain framework and the evolving landscape of cybersecurity including reconnaissance, weaponization, delivery, exploitation, installation, command and control and actions on objectives (Liu et al., 2020) This framework is instrumental in analyzing advanced persistent threats (APTs) and has been utilized to develop detection and defense systems (Liu et al., 2020; syafrizal rt al., 2022).

Recent studies highlight the CKC with various cybersecurity framework such as NIST cybersecurity framework which helps organization in managing cybersecurity risk effectively (Dedeke and Masterson, 2019; Calder, 2018). The literature also highlights the important of adapting the CKC to specific environment such as multimedia service and industrial control system to address unique threat vectors (Kim et al., 2018; Zhou et al., 2018). Furthermore, the application of machine learning techniques in malware detection has gained traction, enhancing the ability to identify and classify malicious software based on behavioral patterns (Alexopoulos and Daras, 2020; Ulven and Wangen, 2021).

## Identification of Key Concepts and Gaps

Key concepts of identified from the literature includes the distinct approaches to malware analysis like static, dynamic and hybrid as well as the stages of the cyber kill chain which includes reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objective. Both areas of research provide critical insight of the detection and repones of cyber threats, but they have largely been developed in isolation.

One of the most significant gaps in the current literature is the lack of comprehensive studies that integrate malware analysis techniques directly into the cyber kill chain framework. While malware analysis has increased with advanced techniques, its application within the cyber kill chain remains underexplored. For example, static and dynamic malware analysis could be applied at different stages of the cyber kill chain static analysis at the reconnaissance or weaponization stage and dynamic analysis at the exploitation or installation stages but there is minimum guidance on how to operationalize such integration (Bahrami et al., 2019).

There are a gap remains in the literature. One major gap is the real validation of the CKC across diverse industries and types of cyber threats limiting its practical applicability (Liu et al., 2020). Additionally, the rapid evolution of malware, particularly with sophisticated avoidance techniques poses ongoing challenges for traditional detection methods, necessitating continuous adaptation of the CKC framework (Suryati and Budiono, 2020; Norouzi et al., 2016). Furthermore, there is a lack of standardized benchmarks for features selection in machine learning models leading to inconsistent results across studies (Liu et al., 2022; Subhash, 2023). Lastly, the integration of emerging technologies such as artificial intelligence and advanced behavioral analysis tools into existing malware detection framework remains underexplored (Kawakoya et al., 2019; Torres et al., 2023). Addressing this gap is crucial for enhancing the resilience of cybersecurity practices in an increasingly complex threat.

## Conclusion of Literature Review

The literature in malware analysis and cyber kill chain (CKC) highlights significant changes in cybersecurity techniques but also reveals key gaps. While static, dynamic, hybrid analyses have proven effectiveness, the integration of these methods within the CKC remains underexplored. The rapid evolution of malware, particularly with evasion techniques, necessitates continuous adaption of detection frameworks. Furthermore, gaps in machine learning features selection and the application of AI in malware detection require further research. Addressing these challenges is essential for improving cybersecurity defenses in an increasingly complex threat landscape.

# Malware Analysis Techniques

Cybersecurity is ever evolving thus enhancing the way malware is analyzed requires constant updates of the methods used. This section describes and evaluates different approaches of malware analysis based on the Cyber Kill Chain model and on it advantages and disadvantages (Al-Janabi and Altamimi, 2020).

A diagram of malware analysis

Description automatically generated

**Figure 1: Types of Malware Analysis**

In sum, realizing the strengths and weaknesses of these techniques, security specialists will be able to choose appropriate methods for the elaboration of protective measures (Al-Marghilani, 2021).

## Static Analysis

In this technique, the code of a malware is analyzed without running the program; it is the primary stage of malware detection. This technique involves as review of the code, the .exe decoding, and the detection of patterns and signatures that are symptomatic of malicious activity. An example is with antivirus software and disassemblers; by identifying static analysis tools, analysts can easily detect known threats and do so in the least amount of time and resources. Static analysis has several advantages; one of which is the ability to easily detect previously identified malware patterns (Pan *et al.* 2020). Security tools such as IDA Pro and Ghidra help in analyzing the code and discover concealed instructions and intents of the program. This approach is best suited for the identification of malware that abuses standard patterns or signatures and therefore serves as accurate quick scan and remediation tool. Nevertheless, static analysis has its drawbacks, especially, in case of polymorphic and metamorphic viruses. The presence of these malwares means that not all of it will be discovered and this minimizes the usefulness of static analysis. Consequently, malware authors often use code obfuscation which is rather a daunting task for static analysis tools. In addition, static analysis can leave inapparent environmental factors that affect the behavior of malware, including conditions at runtime and interactions with other components of the system (Ngo *et al.* 2020).

## Dynamic Analysis

Dynamic analysis in some ways complements some of the limitations of static analysis by running malware in a constrained environment such as a sandbox. This technique helps analysts to view the activity of the malware, or its interaction with the file system, the network, or other processes. Dynamic analysis also gives important observations on the conduct of the malware, for example, copying data to other people, altering systems, and communicating in the network. The main strength of dynamic analysis is in its capacity to ascertain the real behavior of malware, which is important in assessing the effect of a virus and possible ways of dealing with it. There exist open-source solutions that provide isolated environments for running samples of malware, for its behavioral analysis, Cuckoo Sandbox, and FireEye are examples of sandboxing solutions. As a result, dynamic analysis that captures interactions and modifications as it occurs assists in understanding the full potential of malware and the effects it might have on systems. However, dynamic analysis is expensive and requires much time in comparison with other types of analysis because to implement it is necessary to use powerful computers and create complex sandboxes.

## Hybrid Analysis

A more complete approach is to associate aspects of the static analysis with aspects of the dynamic analysis resulting in HYBRID analysis. The approach makes it possible for the analysts to be able to take advantage of the fast and accurate results of a static analysis but at the same time, get more information from dynamic analysis (Ding *et al.* 2021). Consequently, depending on the results of both techniques the hybrid analysis provides a more objective view upon the capabilities and the intentions of the malware. The advantage of hybrid analysis is that this method can identify threats of various levels of familiarity – from those, which are already know by the system and classified as potential dangers, to new threats that were not previously identified as potential dangers by the system. Hybrid of both signatures based, and behavior-based analysis can help to detect new variants of malware that might have slipped through detector of either static or dynamic analysis (Surendran, Thomas et al ,2020).

## Malware Analysis Techniques Comparison

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Malware Analysis Techniques** | **Effectiveness** | **Use Cases** | **Strengths** | **Limitation** |
| **Static Analysis** | High for known malware, less effective against polymorphic/mutation malware. | Quick detection of known malware through signature patterns. | Fast requires fewer resources identifies known patterns. | Ineffective against obfuscated, polymorphic, or metamorphic malware. |
| **Dynamic Analysis** | Effective against complex, evasive malware but resource intensive. | Behavioral analysis to detect unknown or advanced malware. | Reveals real time behavior, effective against unknown malware. | Time consuming, resource heavy, can be evaded by anti-analysis techniques. |
| **Hybrid Analysis** | Combines strengths of both static and dynamic offering more comprehensive detection. | Provides through analysis useful for detection advanced threats. | Covers both code and behavior, balance speed and depth. | Resource intensive and more complex than using static or dynamic alone. |

## Machine Learning and Artificial Intelligence in Malware Analysis

The application of machine learning and artificial intelligence in malware analysis has emerged as a transformative approach to enhancing cybersecurity measures against increasingly sophisticated threats. ML techniques enable the development of models that can learn from vast datasets of malware samples, allowing for the identification and classification of malicious software without relying solely on traditional signatures-based methods. For instance, researchers have demonstrated the effectiveness of various ML algorithms including support vector machine and ensemble methods in detecting malware by analyzing specific features extracted from executable files (Amer and Aziz 2019; Azeez et al., 2021). Additionally, deep learning models such as convolutional neural networks (CNNs) and recurrent neural network (RNNs) have shown promise in recognizing patterns in malware behavior and characteristics particularly in dynamic environments (Fallah and Bidgoly, 2022; Naeem, 2023). These advanced models can adapt to concept drift a common challenge in malware detection where the nature of malware evolves rapidly (Hu et al., 2017). Furthermore, the integration of explainable AI techniques allows for greater transparency in decision making processes helping security analysts understand the rational behind specific classifications (Vanjire, 2024). Overall, the incorporation of ML and AI into malware analysis not only improves detection rates but also enhances the ability to respond to emerging threats making it a critical component of modern cybersecurity strategies.

A diagram of a diagram

Description automatically generated

**Figure 2: Machine Learning in Malware Detection.**

Figure 2 shows the flow of machine learning application in malware detection Beginning with data collection and moving through the features extraction, model training and final detection of malware.

## Relevance to the Cyber Kill Chain

The role of malware analysis techniques in the context of the Cyber Kill Chain is established by the fact that these techniques help to improve the identification and elimination of threats in any of the available chain steps. The integration of such techniques ensures that security specialists have a broader perspective of the lifecycle of an attack and a better response mechanism in the Cyber Kill Chain.

For instance, static analysis can be applied during reconnaissance and weaponization phases of the Cyber Kill Chain model, which are on the detection of threats and threats’ vectors, respectively. Dynamic analysis can be used at the delivery and the exploitation of the life cycle stages where the activities of the malware can be studied. It is important to note that there is no restriction on the implementation of hybrid analysis techniques and machine learning across the complete Cyber Kill Chain, and such continuous monitoring and detection are possible. These techniques provide broad-spectrum approach to analyzing and managing malware, boosting the general security and protection.

# Integration of Malware Analysis Techniques into the Cyber Kill Chain

As a result, it is important to apply the methods of malware analysis in the framework of the Cyber Kill Chain in order to improve its efficiency. In each step of the Cyber Kill Chain, there is a chance to use one or another method of malware analysis to identify and disarm threats. This section investigates the applicability of the techniques described throughout this paper within each of the stages at the level of the Cyber Kill Chain and the advantages and disadvantages of applying it as well as the suggestions for its improvement. The figure 3 shows the cyber kill chain framework It comprises seven distinct phases: reconnaissance, weaponization, delivery, exploitation, installation, command and control, and action on objectives.

A diagram of a chain

Description automatically generated

**Figure 3: Lockheed Martin Cyber Kill Chain** (Bahrami et al., 2019)

## Reconnaissance Stage

In the reconnaissance stage, the assaulter gathers as much information as possible on the target to have weak points to exploit. The integration of static analysis at this stage enables security team to go through potentially injected malicious codes, scripts, configurations files for review without running it (Ju et al., 2020). Static analysis can detect known malware signature, it can alert at the onset of reconnaissance phase. Moreover, the application of machine learning algorithms can improve reconnaissance identification by means of traffic and users’ activity examination. Programs can detect changes and trends that are most likely reconnaissance operations, different from other activities. For example, the clustering algorithm can identify some specific scanning pattern or some queries to the data base which indicates start of an attack (Mekdad *et al.* 2021).

## Weaponization Stage

During the weaponization stage, the attacker develops malicious programmers capable of exploiting the disclosed openings. Static analysis is important here because it enables the analysts to study the structure and the patterns of the malware code. Analyzing statics of malware binaries is possible by means of disassemblers and decompiles; in this way, it is easy to investigate evil intentions and capabilities (Mirza *et al.* 2021). Dynamic analysis is an extension of the static methods in that the analyst runs the malware within a controlled environment to see how it behaves. This makes it possible to establish the log of the activity of the malware in the system; the files created, the registry editing, and network connection made by the malware to the system. Static analysis gives information about the internal functioning of the malware and dynamic analysis gives real time working of the malware possibilities so the two techniques in combination make a total approach and it is seen that about the working of the malware to its full extent.

## Delivery Stage

Transmission of the actual weaponized payload to the target system is done in the delivery stage (Kawakoya et al., 2019). Dynamic analysis is especially important in the task of tracking the delivery vehicles, for example file attachments or network connections (Goss, 2024). It means that Dale’s security teams can define these delivery methods in a sandbox environment, and block the malicious content from reaching the target. Machine learning models take delivery detection a notch higher by categorizing the files and network packets in queues using patterns that have been learned. These models can help identify anomalies within attachments in emails, or even in traffics in the networks, increasing the chances of threat identification. For example, supervised learning models can be trained to detect specific features of known malware; this way, such programs can be evaluated and reacted to quickly.

## Exploitation Stage

The exploitation stage involves malwares chancing a vulnerability then infiltrating the target system illicitly. This is important for dynamic analysis to be done in real time during this phase to see how the malware indulges in such vulnerabilities. Whenever security such changes as the privilege escalation or unauthorized access occurred, it becomes easier for the security teams to detect the exploitation attempts. Furthermore, algorithms of machine learning could be also helpful in identifying the activities connected with exploitation. Anomaly detection models perform the task of comprehending logs and traffic data to recognize activities, which are suspicious and may be a sign of an attempt to exploit a vulnerability. These models can be taught to pick up indicators of exploitation like; unusual systemic commands or unauthorized network connections. This becomes possible so that there can be early identification of various exploitation activities hence improving on the general capacity to counter various potential threats and mitigate on instances of successes by threats that may occur.

## Installation Stage

During the installation phase, malware makes itself fully subordinate to the target system in order to maintain access. It is during this phase that the changes made by the malware to the system must be captured with the help of dynamic analysis this includes creation of new files, modifications to the registry and new scheduled tasks (Kaur and Singh, 2016). Through such dynamic changes, a security team can then take specific steps in eradicating the malware besides severing its operations. Incorporating static and dynamic analysis methods provides improved examined possibilities of persistence mechanisms and backdoors used by the malware. This includes the static information about it with references to its code, structure and dynamics, including the effects that it exercises upon the system operations. Together with the following information, it will be possible to create much more efficient removal and prevention methods which eliminate the malware and guarantee the absence of a possibility to infect a system in future.

## Command and Control (C2) Stage

The final stage of the malware and attacks is the command and controls stage in which the malware communicates with the attacker’s server. Dynamic analysis facilitates monitoring of the network traffic as a way of identifying C2 communication. Analyzing the behavior of malware in the sandbox allows security teams to discover connections to the specific C2 servers, being either already malicious or, potentially, suspicious (Haider, 2024). It also applies for C2 activity detection, with the help of machine learning models. These models can study traffic flow of the network and detect anomalous flow, which may point to presence of C2 communications. Thus, through the learning process of new data, one can enhance its detection capacity and issue alerts on C2 activity (Kim et al., 2022).

## Actions on Objectives Stage

In the actions on objectives stage, the objectives set earlier are achieved, that can be data leakage or systems’ damage. The dynamic analysis serves for the monitoring of the system with regard to illicit activities like data espionage or unauthorized system hopping. If security teams are only notified once a threat starts actively infecting the systems on which malware will operate, these teams can at least watch the activity in real time and apply containment measures to limit the consequences of the attack. Combined methods of analysis which are based on the combination of static and dynamic results provide a multi-layered picture of actions and further intentions of the malware. It also provides a way to recognize the various intricate patterns in an attack and the formulation of an ideal response to these patterns.

## Malware Analysis Techniques into Cyber Kill Chain Stages

|  |  |  |
| --- | --- | --- |
| **Cyber Kill Chain Stages** | **Analysis Techniques** | **Description** |
| **Reconnaissance** | Static Analysis and Machine Learning | Review potentially injected malicious code and configuration without execution. Machine learning detects traffic changes and trends typical of reconnaissance. |
| **Weaponization** | Static Analysis and Dynamic Analysis | Analyze malware binaries (static). Dynamic analysis observes malware behavior in a controlled environment to establish log activity. |
| **Delivery** | Dynamic Analysis and Machine Learning | Track delivery vehicles (network connections) in a sandbox. Machine learning detects anomalies in network traffic and attachments. |
| **Exploitation** | Dynamic Analysis and Machine Learning | Dynamic analysis detects exploitation of system vulnerabilities. Machine learning identifies unusual activities such as unauthorized network connections. |
| **Installation** | Static and Dynamic Analysis | Track changes made to the system (e.g., registry modification). Combined static and dynamic analysis detect persistence mechanisms and backdoors. |
| **Command and Control (C2)** | Dynamic Analysis and Machine Learning | Monitor network traffic for C2 communication. Machine learning detects anomalous network flow potentially indicating C2 activity. |
| **Action on Objective** | Dynamic and Combined Analysis | Monitor system activities related to data theft or system damage. Combined static and dynamic provides a detailed view of malware behavior. |

## Challenges and Opportunities

Incorporation of the malware analysis into the Cyber Kill Chain strikes some of the keys pros and cons. Among it is the problem of automation and scalability. Software solutions for cyber defense have to process great amounts of information that describes ever changing threats. In particular, the concern is to minimize the need for manual analysis techniques and improve the detection performance through automation and machine learning. Another is the issue of how to ensure methodological consistency as well as cooperation between the Organisations. Different methodologies and terminologies used in handling malware are likely to cause disparity in the utilization and implementation of the strategies in malware analysis. Setting best practices as well as cooperation can help to enhance the results of the malware analysis and management of the incident reactions. However, it needs to be mentioned that with these challenges, use of malware analysis techniques in integration with the Cyber Kill Chain presents certain distinct prospects for improving the approaches to the containment of present-day threats. With these techniques matched to each of the phases in the Cyber Kill Chain, security personnel will have a much better way of comprehensively understanding the life cycle of a cyber-attack and thus develop better countermeasures. This integration also help in the identification of the threats at an early stage and also help in’s the implementation of the proactive strategies to the ever changing threats.

# Conclusion

In Conclusion, this research highlights the critical role of malware techniques in enhancing cybersecurity particularly through their integration with the cyber kill chain (CKC). Static, dynamic, hybrid analysis techniques each offers unique advantages and limitation with hybrid methods showing promise for more comprehensive detection. However, their integration with the CKC remains underdeveloped. The rapid evolution of malware especially in terms of evasion techniques necessitates continuous adaptation of detection framework and strategies. Additionally, the lack of standardization in machine learning features selection and the limited empirical validation of the CKC across diverse industries represent significant gaps. Addressing these challenges through further research and innovation will be essential for strengthening cybersecurity defenses and improving resilience against increasing sophisticated cyber threats.

# References

1. Liu, C., Singhal, A. and Wijesekera, D., 2020. Forensic analysis of advanced persistent threat attacks in cloud environments. In *Advances in Digital Forensics XVI: 16th IFIP WG 11.9 International Conference, New Delhi, India, January 6–8, 2020, Revised Selected Papers 16* (pp. 161-180). Springer International Publishing.
2. Ahmed, Y., Asyhari, A.T. and Rahman, M.A., 2021. A cyber kill chain approach for detecting advanced persistent threats. *Computers, Materials and Continua*, *67*(2), pp.2497-2513.
3. Huang, R., Ma, R. and Zhang, H., 2024, July. Agricultural IoT PDRR scheme based on an improved cyber kill chain. In *International Conference on Signal Processing and Communication Security (ICSPCS 2024)* (Vol. 13222, pp. 83-90). SPIE.
4. Rashid, S.H. and Abdullah, W.D., 2023. Enhanced website phishing detection based on the cyber kill chain and cloud computing. *Indonesian Journal of Electrical Engineering and Computer Science*, *32*(1), pp.517-529.
5. Rieck, K., Trinius, P., Willems, C. and Holz, T., 2011. Automatic analysis of malware behavior using machine learning. *Journal of computer security*, *19*(4), pp.639-668.
6. Bayer, U., Kirda, E. and Kruegel, C., 2010, March. Improving the efficiency of dynamic malware analysis. In *Proceedings of the 2010 ACM Symposium on Applied Computing* (pp. 1871-1878).
7. Shosha, A.F., James, J.I., Hannaway, A., Liu, C.C. and Gladyshev, P., 2013. Towards Automated malware behavioral analysis and profiling for digital forensic investigation purposes. In *Digital Forensics and Cyber Crime: 4th International Conference, ICDF2C 2012, Lafayette, IN, USA, October 25-26, 2012, Revised Selected Papers 4* (pp. 66-80). Springer Berlin Heidelberg.
8. Talukder, S. and Talukder, Z., 2020. A survey on malware detection and analysis tools. *International Journal of Network Security & Its Applications (IJNSA) Vol*, *12*.
9. Liu, K., Xu, S., Xu, G., Zhang, M., Sun, D. and Liu, H., 2020. A review of android malware detection approaches based on machine learning. *IEEE access*, *8*, pp.124579-124607.
10. Shijo, P.V. and Salim, A.J.P.C.S., 2015. Integrated static and dynamic analysis for malware detection. *Procedia Computer Science*, *46*, pp.804-811.
11. El Merabet, H. and Hajraoui, A., 2019. A survey of malware detection techniques based on machine learning. *International Journal of Advanced Computer Science and Applications*, *10*(1).
12. Aboaoja, F.A., Zainal, A., Ghaleb, F.A., Al-Rimy, B.A.S., Eisa, T.A.E. and Elnour, A.A.H., 2022. Malware detection issues, challenges, and future directions: A survey. *Applied Sciences*, *12*(17), p.8482.
13. Kumar, R., Alenezi, M., Ansari, M.T.J., Gupta, B., Agrawal, A. and Khan, R.A., 2020. Evaluating the impact of malware analysis techniques for securing web applications through a decision-making framework under fuzzy environment. *Int. J. Intell. Eng. Syst*, *13*(6), pp.94-109.
14. Moneva, A., Ruiter, S. and Meinsma, D., 2024. Criminal expertise and hacking efficiency. *Computers in Human Behavior*, *155*, p.108180.
15. Kong, G., Chen, F., Yang, X., Cheng, G., Zhang, S. and He, W., 2023. Optimal Deception Asset Deployment in Cybersecurity: A Nash Q-Learning Approach in Multi-Agent Stochastic Games. *Applied Sciences*, *14*(1), p.357.
16. Syafrizal, M., Selamat, S.R. and Zakaria, N.A., 2020. Analysis of cybersecurity standard and framework components. *International Journal of Communication Networks and Information Security*, *12*(3), pp.417-432.
17. Dedeke, A. and Masterson, K., 2019. Contrasting cybersecurity implementation frameworks (CIF) from three countries. *Information & Computer Security*, *27*(3), pp.373-392.
18. Calder, A., 2018. *NIST Cybersecurity Framework: A pocket guide*. IT Governance Publishing Ltd.
19. Kim, H., Kwon, H. and Kim, K.K., 2019. Modified cyber kill chain model for multimedia service environments. *Multimedia Tools and Applications*, *78*, pp.3153-3170.
20. Zhou, X., Xu, Z., Wang, L., Chen, K., Chen, C. and Zhang, W., 2018. Kill chain for industrial control system. In *MATEC Web of Conferences* (Vol. 173, p. 01013). EDP Sciences.
21. Alexopoulos, A. and Daras, N., 2020. Mathematical Study of Advanced Persistent Threat (APT) Hunting Techniques. *Journal of Computations & Modelling*, *10*(2), pp.1-24.
22. Ulven, J.B. and Wangen, G., 2021. A systematic review of cybersecurity risks in higher education. *Future Internet*, *13*(2), p.39.
23. Bahrami, P.N., Dehghantanha, A., Dargahi, T., Parizi, R.M., Choo, K.K.R. and Javadi, H.H., 2019. Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures. *Journal of information processing systems*, *15*(4), pp.865-889.
24. Suryati, O.T. and Budiono, A., 2020. Impact analysis of malware based on call network API with heuristic detection method. *International Journal of Advances in Data and Information Systems*, *1*(1), pp.1-8.
25. Norouzi, M., Souri, A. and Samad Zamini, M., 2016. A data mining classification approach for behavioral malware detection. *Journal of Computer Networks and Communications*, *2016*(1), p.8069672.
26. Liu, Y., Li, J., Liu, B., Gao, X. and Liu, X., 2022. Malware detection method based on image analysis and generative adversarial networks. *Concurrency and Computation: Practice and Experience*, *34*(22), p.e7170.
27. ubhash, P., Varsha, Y.S., Reddy, K.S., Akshaya, B. and Kalyani, S., 2023, December. Visual Profiling and Automated Classification of Malware Samples using Deep Learning. In *Proceedings of the Fourth International Conference on Advances in Computer Engineering and Communication Systems (ICACECS 2023)* (Vol. 18, p. 249). Springer Nature.
28. Torres, M., Álvarez, R. and Cazorla, M., 2023. A Malware Detection Approach Based on Feature Engineering and Behavior Analysis. *IEEE Access*.
29. Pan, Y., Ge, X., Fang, C. and Fan, Y., 2020. A systematic literature review of android malware detection using static analysis. IEEE Access, 8, pp.116363-116379.
30. Ngo, Q.D., Nguyen, H.T., Le, V.H. and Nguyen, D.H., 2020. A survey of IoT malware and detection methods based on static features. ICT express, 6(4), pp.280-286.
31. Ding, C., Luktarhan, N., Lu, B. and Zhang, W., 2021. A hybrid analysis-based approach to android malware family classification. Entropy, 23(8), p.1009.
32. Surendran, R., Thomas, T. and Emmanuel, S., 2020. A TAN based hybrid model for android malware detection. Journal of Information Security and Applications, 54, p.102483.
33. Amer, A. and Aziz, N.A., 2019. Malware detection through machine learning techniques. *International Journal of Advanced Trends in Computer Science and Engineering*, *8*(5), pp.2408-2413.
34. Azeez, N.A., Odufuwa, O.E., Misra, S., Oluranti, J. and Damaševičius, R., 2021, February. Windows PE malware detection using ensemble learning. In *Informatics* (Vol. 8, No. 1, p. 10). MDPI.
35. Fallah, S. and Bidgoly, A.J., 2022. Android malware detection using network traffic based on sequential deep learning models. *Software: Practice and Experience*, *52*(9), pp.1987-2004.
36. Naeem, H. and Batool, A., 2023. Malware Attacks Detection in Network Security using Deep Learning Approaches. *International Journal for Electronic Crime Investigation*, *7*(3), pp.35-48.
37. Hu, D., Ma, Z., Zhang, X., Li, P., Ye, D. and Ling, B., 2017. The concept drift problem in Android malware detection and its solution. *Security and Communication Networks*, *2017*(1), p.4956386.
38. Vanjire, S.S. and Lakshmi, M., 2024. A novel method of detecting malware on Android mobile devices with explainable artificial intelligence. *Bulletin of Electrical Engineering and Informatics*, *13*(3), pp.2019-2026.
39. Ju, A., Guo, Y. and Li, T., 2020. MCKC: a modified cyber kill chain model for cognitive APTs analysis within Enterprise multimedia network. Multimedia Tools and Applications, 79(39), pp.29923-29949.
40. Maniriho, P., Mahmood, A.N. and Chowdhury, M.J.M., 2022. A study on malicious software behaviour analysis and detection techniques: Taxonomy, current trends, and challenges. Future Generation Computer Systems, 130, pp.1-18.
41. Mekdad, Y., Bernieri, G., Conti, M. and Fergougui, A.E., 2021, May. A threat model method for ICS malware: the TRISIS case. In Proceedings of the 18th ACM International Conference on Computing Frontiers (pp. 221-228).
42. Mirza, Q.K.A., Brown, M., Halling, O., Shand, L. and Alam, A., 2021, August. Ransomware analysis using cyber kill chain. In 2021 8th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 58-65). IEEE.
43. Kaur, R. and Singh, M., 2016. Hybrid real-time zero-day malware analysis and reporting system. *Int. J. Inf. Technol. Comput. Sci*, *8*, pp.63-73.
44. Goss, A. (2024) The Cyber Kill Chain: How To Map And Analyze Cyber Attacks - Kraven Security. *Kraven Security*. <https://kravensecurity.com/cyber-kill-chain/>.
45. Kawakoya, Y., Shioji, E., Iwamura, M. and Miyoshi, J., 2019. Api chaser: Taint-assisted sandbox for evasive malware analysis. *Journal of Information Processing*, *27*, pp.297-314.
46. Haider, R.Z., Aslam, B., Abbas, H. and Iqbal, Z., 2024. C2-Eye: framework for detecting command and control (C2) connection of supply chain attacks. *International Journal of Information Security*, pp.1-15.
47. Kim, Y.J., Park, C.H. and Yoon, M., 2022. Film: Filtering and machine learning for malware detection in edge computing. *Sensors*, *22*(6), p.2150.
48. Zhang, Z., Qi, P. and Wang, W., 2020, April. Dynamic malware analysis with feature engineering and feature learning. In Proceedings of the AAAI conference on artificial intelligence (Vol. 34, No. 01, pp. 1210-1217).