Achieving Consistency and Efficiency in Malware Analysis

A Research Project for the Naval Information Warfare Center Internship Program

by

Kye Steele

May 2023

Abstract

The nonstop evolution of malware presents the need for developing and improving current mitigation and prevention techniques. Disrupting malware has been a significant and complex problem facing both the security community and the world. The study will provide an overview of the evolution of malware and its analysis, the current counter-operation methods, and suggested changes in order to obtain better consistency and efficiency. It aims to give valuable insight for the researchers, law enforcement, and the security community and shed light on different possibilities that bring us closer to a full-fledged solution. The study is intended to fill the gaps between the current research and techniques or strategies used. The findings result in the suggested changes as follows: limiting time per sample in sandbox analysis, moving to a one class triage method, and more consideration of the history and trends of malware itself. For future work, it is advised that researchers consider the suggested changes but ultimately adapt them to further develop current and future techniques and strategies.

Table of Contents

Section 1: Introduction

Since before the 1980s, malware has historically been utilized to obtain publicly restricted information, access or take over computer systems, and disrupt operations of computer systems (Milosevic, 2013). As the internet and technology have evolved, computer systems and the data stored on them as well as their capabilities are more sensitive than ever (Alenezi et al., 2020). Consequently, cybercriminal operations have also evolved rapidly, particularly in how malware can be used as an attack method (Alenezi et al., 2020). The current malware industry has become a source of mass profits for criminals and is becoming more and more complex for both the security community and the world (Alenezi et al., 2020). A current technique commonly used to analyze malware is known as "dynamic" analysis, where analysts can directly observe the behavior of malware in a controlled environment (Afianian et al., 2018). Additional necessary processes are malware triage and classification when determining the priority of analysis (Ucci et al., 2018). Malware is always evolving so it is the goal of researchers to find ways to get ahead of the attackers in preventing and mitigating impacts, so it can be inferred that several changes to current techniques will need to be made (Ife et al., 2021).

Problem Statement

Due to the rapid evolution of malware, there is a need for researchers, law enforcement agencies, and security companies to use better prevention and mitigation techniques to disrupt malicious operations (Ife et al., 2021). Dealing with malware has been a prominent issue in the security community and the world as it grows rapidly both in sheer volume as well as complexity (Ucci et al., 2018). The methods of delivery for such malware have evolved as the years passed and are now

considered to be a substantial business in the network and economy of cyber-criminals (Ife et al., 2021). Through this recent evolution, the need for researchers to develop better solutions has been exemplified (Lee, 2019). That is, to change the current solutions to obtain more consistent results. An example of this is the use of "sandboxes" to analyze malware and the goal to make the process as efficient and effective as possible. (Kuchler et al., 2021). Another goal is finding the optimal balance between efficiency and accuracy when classifying malware (Ucci et al., 2018). Since malware is continuing to evolve, it is arguably crucial for the development and adaptation of current prevention and mitigation techniques using prior findings related to malware behavior.

Study Purpose

The purpose of the study is to provide valuable insight for the security community, law enforcement, and fellow researchers. Specifically, to further improve or develop new strategies for counter-operations regarding malware (Lee, 2019). The study attempts to connect priorly conducted malware analysis research to how current prevention/mitigation techniques and strategies can be improved, potentially resulting in more consistent results from counter-operations (Ife et al., 2021).

Research Question

How can current malware prevention and mitigation techniques be improved, or changed such that it would result in more consistent counter-operations? This study aims to answer this question and offer insight to the security community that will help mitigate this issue.

Significance of the Study

This study hopes to fill the gaps within the current research on malware mitigation and prevention techniques. It will provide insight into the suggested changes to be made, what areas to focus on, and what to do next. Recently conducted research from respected professionals will be analyzed to find ways to obtain more consistent and reliable solutions directly related to malware mitigation and prevention. Readers from the security community should have valuable takeaways from

this study that can be applied, and it is suggested that the research provided in this study be used for the future development of strategies and techniques. It can be argued that learning from current research is crucial for getting ahead of cybercriminals in this ever-evolving cat-and-mouse game.

Definition of Terms

The following terms will be used within the literature review below. These terms are as follows: botnet, ClamAV, dynamic analysis, malware, ransomware, rootkits, sandbox, static analysis, Stuxnet, and Yara. This section provides the definitions for your understanding such that the literature review can be read to its fullest extent.

Botnet.

The botnet is described as a network of devices infected by malware, controlled by a single attacker, through command-and-control servers (Ife et al., 2021).

ClamAV.

ClamAV is an anti-virus engine used in malware detection, identification, and classification (Jaramillo, 2018).

Dynamic Analysis.

Dynamic analysis refers to a newer method of malware analysis, where researchers can see behaviors in real-time from a controlled environment (Afianian et al., 2018).

Malware.

Malware is defined as malicious software that can be used to access unauthorized systems or information (Milosevic, 2013).

Ransomware.

Ransomware is a specific category of malware that encrypts the information on a system and requires a ransom fee to decrypt this information (Milosevic, 2013).

Rootkits.

Rootkits are a type of malware that alters an infected system such that the malware can remain undetectable (Milosevic, 2013).

Sandbox.

The sandbox is a controlled environment for testing and analyzing malware. It is used in dynamic malware analysis described above (Afianian et al., 2018).

Static Analysis.

Static analysis refers to a method of malware analysis in which researchers analyze the source code of malware (Lee, 2019).

Stuxnet.

Stuxnet is a type of malware that has been used to disrupt Iranian nuclear programs (Milosevic, 2013).

Yara.

Yara is a tool used by malware analysts to classify samples of malware and uses user-created rules to detect and prevent attacks (Jaramillo, 2018).

Section Summary

Malware is always evolving which results in the need for researchers to develop better methods to cope with these changes. This study aims to give insight into how these methods should be developed and what should be taken into account going forward. It is believed by connecting recently conducted research to each other, more consistent and efficient solutions can be achieved.

Section 2: Review of the Literature

The increasing volume and complexity of malware due to its everlasting evolution proves to be a complex problem (Ucci et al., 2018). This study aims to provide insight to generate more consistent results (Ife et al., 2021). It is built upon previous research from a multitude of journals, studies, and other findings from researchers across the world.

Literature Search Strategies

The literature search was conducted primarily through Google Scholar. Key phrases and words include the following: malware analysis, malware evolution, malware history, malware counter-operations, malware sandbox, malware detection, malware identification, and malware classification. Each source was reviewed prior to citation to determine how recent the article was and if it were an older publication an evaluation of its significance was performed. To avoid paywalls, a simple google search often revealed a free pdf copy, which was confirmed to be the same material.

Evolution of Malware

The term malware refers to various intrusive or hostile software, including viruses, spyware, and more (Alenezi et al., 2020). The history of malware is typically spread across five main phases (Milosevic, 2013). The first phase refers to the early introduction and development of malware (Milosevic, 2013). John Von Neumann is the first virus developer when he created the “self-replicating string of code” in the year 1949 (Alenezi et al., 2020). After this initial uprise, Microsoft released Windows, leading to a variety of Windows-based malware such as WinVir, the first-ever virus for Windows (Milosevic, 2013). When the internet became more and more popular, the development of network worms began (Milosevic, 2013). Network worms are a type of malware that scans a network and looks for ways to gain access to and exploit a computer (Milosevic, 2013). The fourth phase refers to the introduction of Rootkits, malware that alters a system such that criminals can continue to access a

machine without being noticed, as well as ransomware, which encrypts a user's data and demands a ransom fee be paid to decrypt it (Milosevic, 2013). The most recent phase of malware deals with sabotage and espionage and the concept of malware being used as a weapon (Milosevic, 2013). Malware has evolved to the point that the US government sees it as an equal threat to that of a bomb (Milosevic, 2013). For instance, malware known as Stuxnet was developed to eliminate or delay an Iranian nuclear program (Milosevic, 2013). Stuxnet exemplifies the evolution of malware operations in that it used RootKit to remain undetectable while spreading to different PCs via USB sticks (Milosevic, 2013). Physically speaking, it was able to change the rotation frequencies of turbines being used for uranium enrichment (Milosevic, 2013). More recently, the evolution of the botnet has become a major issue because of the diversity in its distribution vectors (Ife et al., 2021). Although malware was originally not meant to cause any harm, it is evident that the recent exponential growth and evolution is a cause for concern (Alenezi et al., 2020).

Counter-Operations Methods

To further understand, mitigate, and disrupt malware operations, one can analyze the malware itself with a variety of available tools. A large part of malware analysis has to do with identifying and classifying it (Jaramillo, 2018). ClamAV is an anti-virus engine that can be used for detecting malware as code or artifacts (Jaramillo, 2018). After malware is detected, the next phase is identification and classification (Jaramillo, 2018). Malware analysts use tools like Yara to classify samples of malware since it allows the user to create custom rules to detect/prevent attacks (Jaramillo, 2018). The coding style of the malware can also be analyzed to reveal information on the original developer's identity (Ucci et al., 2018). The code is profiled based on syntax, lexicon, and layout, but in practice, this method is not used often due to the need for available source code (Ucci et al., 2018). This concept of attribution in the modern era is being developed with machine learning, but researchers must find other ways to obtain "ground truth" rather than an educated guess (Ucci et al., 2018).

In the classification of malware, the samples typically undergo a "triage" (Ucci et al., 2018). The reason for this is that countermeasures need to be deployed faster than malware can evolve, requiring some system of prioritization (Laurenza et al., 2020). Due to the large number of new samples, each new sample is compared to known samples (Ucci et al., 2018). The more similar the samples, the less of a priority examination is (Ucci et al., 2018). If the new sample is very different from known malware, further examination is advised and prioritized (Ucci et al., 2018). A complex problem presented by the malware triage method is finding the optimal balance of accuracy and performance (Ucci et al., 2018). Malware analysis can be divided into two main categories: static and dynamic analysis (Afianian et al., 2018). Static analysis refers to looking at code or binary on its own, without running anything (Afianian et al., 2018). On the other hand, dynamic analysis is analyzing the behavior of malware as it is being executed (Afianian et al., 2018). Both are done either manually, by experts, or automatically via some machine (Afianian et al., 2018).

There are a multitude of techniques within static analysis when assessing malware behavior (Lee, 2019). Although they may be useful, a recent trend known as file-less malware thwarts this forensic method since the malware is completely within the memory of a system and not the storage (Afianian et al., 2018). Essentially, malware developers have learned the drawbacks of static analysis and can exploit them (Lee, 2019). Another drawback is that outputs may not be the same as the actual behavior when the malware is executed, since many times it is impossible to accurately see what will happen from pure static analysis (Lee, 2019). The solution is for analysts to switch to an entirely different method, known as dynamic analysis, to overcome these drawbacks (Afianian et al., 2018).

In dynamic analysis, analysts use what is referred to as a "sandbox," which is a controlled environment to test and study malware behavior as it executes (Afianian et al., 2018). It should be noted however that although sandboxes have been researched and developed thoroughly, it is still a mystery when it comes to optimizing them (Kuchler et al., 2021). The main benefit of dynamic analysis is that it is

effective for any type of malware since any and all malware executes similarly and thus can be analyzed similarly as well (Lee, 2019).

Achieving Consistency and Efficiency

With sandboxes being a prominent and commonly used solution for malware analysis, researchers aim to not only get meaningful results but to do so efficiently (Kuchler et al., 2021). In a study conducted at the University of Mannheim, Willems, and his peer researchers state, “We found that executing the malware for two minutes yielded the most accurate results...” (2007). This report is then built upon by researchers from Fraunhofer, EURECOM, and NortonLifeLock, who found that most malware samples execute either under two minutes or longer than ten (Kuchler et al., 2021). In other words, for almost all samples, two minutes is sufficient for accurate and qualitative data in dynamic sandbox analysis (Kuchler et al., 2021). It is noted that although stalling code may be a common analysis evasion technique, it was of negligible impact given that “its most common form (which relies on invoking one of the sleep functions) only affected 2-3%” of the sample pool and that some sandboxes have built-in countermeasures (Kuchler et al., 2021).

When classifying malware, it can be difficult to find a compromise between efficiency and accuracy, thus the use of the triage method (Ucci et al., 2018). It was suggested that triage should be done by comparing new samples to known samples, with priority determined by contrast (Ucci et al., 2018). However, there is a different method suggested by a group of researchers from the University of Rome that will give better results (Laurenza et al., 2020). They state, “Malware developed by known APTs have been detected with precision and accuracy over 90%” (Laurenza et al., 2020). This new method builds upon the previous triage algorithm but moves from a multi-class classifier approach to a one-class classifier approach (Laurenza et al., 2020). As a result, lesser time is needed for manual analysis, allowing for a quicker evaluation and eliminating part of the burden placed on analysts while still providing an accurate analysis (Laurenza et al., 2020).

Conclusions

Malware is always evolving, and it is becoming increasingly more difficult to deal with (Ucci et al., 2018). To combat this evolution, researchers must develop more sophisticated methods, operations, and algorithms (Lee, 2019). The study aims to make the connections between the analysis and understanding of malware to the implemented defenses (Afianian et al., 2018).

Section Summary

Due to the growing complexity of malware, the defense against it should be developed accordingly, and ideally, faster than malware can evolve. That is the need for more efficient malware analysis which comes with the improvement of sandbox/dynamic analysis, faster triage algorithms like the APT-triage method, and more. The history and trends of malware should be considered when improving upon the current counter-operation methods.

Section 3: Findings

An analysis of the evolution and current trends of malware can be used to achieve more consistent and efficient techniques and strategies. That is, to provide insight to law enforcement, the security community, and researchers when improving these techniques. The rapid evolution of malware results in the need for improvement of current strategies and techniques regarding mitigation and prevention.

Results

An analysis of the history of malware in a short time frame exemplifies the concept that malware is evolving rapidly. However, it can also be seen that criminals are not the only ones making use of this attack method. A direct example of this is Stuxnet, where malware was developed and used by the United States Secret Service to disrupt nuclear operations in Iran (Milosevic, 2013).

It was found that malware analysis, particularly in efficiency, is significantly impacted by the utilized triage and classification methods. Regarding the current triage method, the research suggested a new method with “precision and accuracy over 90%” be used instead (Laurenza et al., 2020). Furthermore, it was also found that transitioning from a multi-class to a single-class approach in the classification of malware results in faster evaluation and less manual labor for similar accuracy (Laurenza et al., 2020).

In malware analysis, studies show that while dynamic analysis is significantly more effective and efficient than static analysis, there are constraints that must be in place for maximum efficiency and practicality (Kuchler et al., 2021). Professor Willems and his team from the University of Mannheim found that running malware for around two minutes gave the most accurate results in the shortest possible amount of time (2007). Kuchler and his team conducted an additional, more refined study and obtained the same results (Kuchler et al., 2021).

Discussion of Study Findings

Given that malware has historically been used by the United States government to achieve its goals, it might be realized that the analysis of malware can be used as a method for developing tools for global cyber-warfare (Milosevic, 2013). Due to the amount of sensitive data stored on computer systems today, it can be argued that malware analysis is crucial in defending a country and its people as a whole (Alenezi et al., 2020).

Current research suggests triage and classification methods be modified or replaced in exchange for efficiency (Laurenza et al., 2020; Ucci et al., 2018). It is observed that when malware is triaged and classified faster, while still being as accurate, it results in a higher volume of malware that can be dealt with (Laurenza et al., 2020; Ucci et al., 2018). This, in turn, helps achieve the goal of getting ahead of cybercriminals. A similar conclusion can be drawn specifying the amount of time spent in malware execution for dynamic analysis in order to obtain results quicker (Kuchler et al., 2021).

Section Summary

Malware has been evolving rapidly since it was first introduced to the world of cyber security. Although primarily used as an attack method by criminals, it is also used by governments (Milosevic, 2013). In hopes of getting ahead of cybercriminals and the evolution of malware, researchers suggest several modifications to the current malware triage, classification, and analysis techniques/strategies (Laurenza et al., 2020; Ucci et al., 2018; Kuchler et al., 2021).

Section 4: Discussion and Conclusions

The evolutionary nature of malware presents the necessity for improved prevention and mitigation techniques (Ife et al., 2021). Furthermore, the improvement will result in more consistent results for the disruption of malicious operations (Lee, 2019). This study was conducted in the hopes that it gives valuable insight to researchers, law enforcement, and the security community. The intent is to connect the existing malware analysis research to the prevention and mitigation techniques used today to achieve the desired improvement in consistency (Ife et al., 2021).

Limitations of Study Findings

Although the study is based upon existing research, it should be noted that only publicly accessible information that was released prior to the study could be used. Malware and its delivery operations are always evolving, so this study's findings may not be the most recent. However, the findings still hold value as it suggests viable modifications to current techniques. There may be some inaccuracy due to the cited studies being conducted at the desired thoroughness of researchers, but their results still hold great significance in solving this complex problem.

Interpretation of Study Findings

The historical usage of malware suggests that improvements in malware analysis will be a worthwhile investment in defending a country along with its people (Alenezi et al., 2020; Milosevic, 2013). It is inferred that moving to a single class triage method will lead to quicker evaluation and allow for less manual labor by analysts (Laurenza et al., 2020). Although the research states a 90% accuracy rating, it would be beneficial to solidify this claim through more testing (Laurenza et al., 2020). In addition, the current research indicates that a maximum two-minute time frame be used in dynamic analysis for optimization (Kuchler et al., 2021). Like the classification modification, it is important to implement the suggestions to see real results.

Practice Implications of Study Findings

The findings of this study are merely the suggested changes to current practices, but it is crucial that analysts implement these changes, adjusting accordingly to build upon this in developing future methods. Ultimately, the goal is to improve current techniques for consistency and efficiency. It is believed that moving to a single class triage method and placing a two-minute time constraint on sandbox analysis will result in this. It is implied that analysts do not need to concretely follow this, but these changes allow for further development of the techniques in practice.

Recommendations for Further Research

Although a two-minute limit on sandbox analysis is recommended, researchers should work on fine tuning this time frame, while still avoiding the unjustified costs of longer times such as five minutes per sample (Kuchler et al., 2021). While fine tuning this time frame, researchers should account for malware that implement certain techniques to delay analysis times and derive their own solutions should they come across this (Kuchler et al., 2021). In addition to a single class approach in malware classification, a suggested future development is growing our current knowledge to account for the many categorizations of malware that are not technically included (Laurenza et al., 2020).

Conclusion

The findings of the study provide feasible and practical suggestions to the current practices, such that we get closer to the maximal optimization of analysis. They also leave room for improvement by researchers in the future, as these changes are further examined and put into practice. Although the findings do not give a concrete way to stop malware as a whole, they do provide valuable insight into getting closer to the desired solution.

References

Afianian, A., Niksefat, S., Sadeghiyan, B., & Baptiste, D. (2018). Malware dynamic analysis evasion techniques: a survey. *ACM Computing Surveys,* https://arxiv.org/pdf/1811.01190.pdf

Alenezi, M., & Alabdulrazzaq, H. (2020). Evolution of malware threats and techniques: a review. *International Journal of Communication Networks and Information Security,* https://www.researchgate.net/profile/Haneen-Alabdulrazzaq/publication/349324759_Evolution_of_Malware_Threats_and_Techniques_A_Review/links/602ad0e64585158939a93934/Evolution-of-Malware-Threats-and-Techniques-A-Review.pdf

Ife, C., Shen, Y., Murdoch, S., & Stringhini, G. (2021). Marked for disruption: tracing the evolution of malware delivery operations targeted for takedown. *International Symposium on Research in Attacks, Intrusions, and Defenses*, *V*(24), 01-13, https://dl.acm.org/doi/pdf/10.1145/3471621.3471844

Jaramillo, L. (2018). Malware detection and mitigation techniques: lessons learned from Mirai DDOS attack. *Journal of Information Systems Engineering & Management,* https://doi.org/10.20897/jisem/2655

Kuchler, A., Mantovani, A., Han, Y., Bilge, L., & Balzarotti, D. (2021). Does every second count? Time-based evolution of malware behavior in sandboxes. *Network and Distributed Systems Security (NDSS) Symposium 2021,* https://www.ndss-symposium.org/ndss-paper/does-every-second-count-time-based-evolution-of-malware-behavior-in-sandboxes/

Laurenza, G., Lazzaretti, R., & Mazzotti, L. (2020). Malware triage for early identification of advanced persistent threat activities. *Digital Threats: Research and Practice,* https://dl.acm.org/doi/pdf/10.1145/3386581

Lee, W. (2019). Malware and attack technologies knowledge area. *The Cyber Security Body of Knowledge,* https://www.cybok.org/media/downloads/Malware__Attack_Technology_issue_1.0.pdf

Milosevic, N. (2013). History of malware. *Digital Forensics Magazine, 58-66,* https://arxiv.org/ftp/arxiv/papers/1302/1302.5392.pdf

Ucci, D., Aniello, L., & Baldoni, R. (2018). Survey of machine learning techniques for malware analysis. *Computers and Security,* https://eprints.soton.ac.uk/426403/1/main.pdf

Willems, C., Holz, T., & Freiling, F. (2007). Toward automated dynamic malware analysis using CWSandbox. *IEEE Security and Privacy,* https://dl.acm.org/doi/10.1109/MSP.2007.45