Undetectable Computer Virus

# Project Report – 2

## Work Done

* Conducted a thorough review of three research papers, extracting information on types of malwares and their camouflaged algorithms.
* Classified malware into different categories based on the extracted data and examined their characteristics.
* Explored the concepts of polymorphic and metamorphic viruses, understanding their code-changing techniques and evasion strategies.
* Reading up on research papers about undetectable computer viruses. This involves understanding the latest tricks and techniques used by cybercriminals to create viruses that slip under the radar.

## Papers Referred:

1. Camouflage In Malware: From Encryption To Metamorphism
   * Babak Bashari Rad, Faculty of Computer Science and Information System, University Technology Malaysia
   * Maslin Masrom , Razak School of Engineering and Advanced Technology, University Technology Malaysia
   * Suhaimi Ibrahim, Advanced Informatics School, University Technology Malaysia
2. Mechanisms of Polymorphic and Metamorphic Viruses

* Xufang Li, Peter K.K. Loh Computer Security Lab Nanyang Technological University Singapore
* Freddy Tan, Microsoft (Asia) and International Information Systems Security Certification Consortium

1. On the Anatomy of the Dynamic Behavior of Polymorphic Viruses
   * Armando Cabrera, College of Technology Purdue University Northwest Hammond, IN, USA
   * Ricardo Calix, College of Technology Purdue University Northwest Hammond, IN, USA

## Summary

Paper1 article explores the evolution of camouflage techniques in malware, including encryption, metamorphism, and obfuscation. It emphasizes the need for antivirus experts to study and analyze these techniques to enhance malware detection.

Paper2 provides an in-depth analysis of polymorphic and metamorphic viruses, which are types of malware that employ obfuscation techniques to avoid detection. The authors discuss the various mechanisms used by these viruses, including encryption, decryption, code transformation, obfuscation, and host code mutation. They also present the structures and characteristics of two specific viruses, W32/Fujacks and W32/Vundo. The paper highlights the significance of detecting and preventing these types of viruses.

While Paper 3 discusses the use of dynamic malware analysis and machine learning techniques to detect polymorphic viruses. The researchers used emulators to generate a dataset of malware and non-malware samples and applied machine learning to create a classifier for polymorphic virus detection. They also explored the challenges of malware analysis and the limitations of static and dynamic analysis techniques.

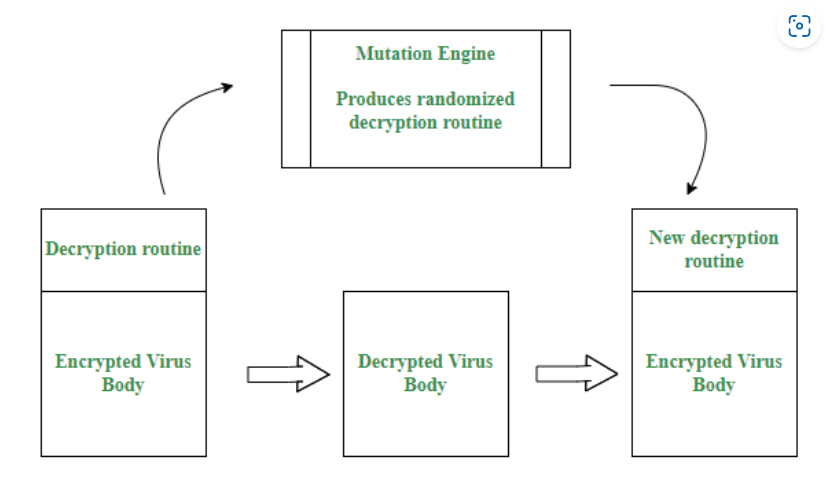
In paper 1, The author categorizes the Malware into 2 types Primitive Malware and Stealth Malware, Stealth malware refers to malicious code that is designed to conceal its presence and evade detection by antivirus software or code analysts. It employs various techniques to hide its signs and traces within the system resources. The term "stealth" is used as a general term for all kinds of malicious codes that are capable of hiding themselves from being visible. The main reasons for using stealth techniques in malware are to make it invisible to non-experts, prevent static analysis and reverse engineering, prolong the lifetime of the virus, and prevent modification of the code by others. Primitive malware, on the other hand, refers to the early forms of malicious code that were created as a kind of programming fun for computer specialists to showcase their technical skills. In the beginning, there were no techniques invented to escape from code analyzers or experts who were trying to find malicious code and trap them. Computer programmers enjoyed finding new ways to demonstrate their programming strengths.

## Camouflages Algorithms

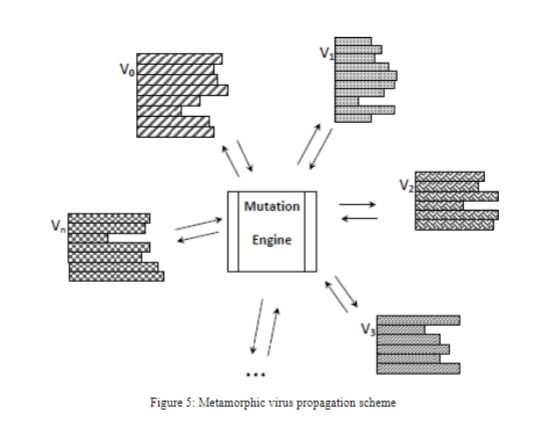
Camouflage algorithms are techniques used by malware creators to hide the presence of malicious code and evade detection by antivirus software. These algorithms employ various methods to obfuscate the code and make it difficult for analysts to identify and analyze the malware [1].

Some common camouflage algorithms include:

1. **Encryption**: This is one of the earliest and simplest methods used by malware programmers. The code is encrypted to make it unreadable and prevent detection by antivirus scanners. The encrypted code is decrypted at runtime to execute the malicious actions.
2. **Oligomorphism**: Oligomorphic malware uses multiple variations of its code to avoid detection. Each variant has a different encryption key or algorithm, making it difficult for antivirus software to identify and block the malware.
3. **Polymorphism**: Polymorphic malware generates new code variants with each infection. The code is modified or mutated in some way, while maintaining the same functionality. This makes it challenging for antivirus software to detect the malware based on static signatures.



1. **Metamorphism**: Metamorphic malware goes a step further by completely rewriting its code with each infection. The new code has the same functionality but looks different, making it extremely difficult to detect and analyze. Metamorphic malware can also employ techniques like code obfuscation and code transposition to further complicate analysis.



These camouflage algorithms are constantly evolving as malware creators find new ways to evade detection. Antivirus software developers need to continually update their detection techniques to keep up with these evolving camouflage algorithms.

## How Polymorphic and Metamorphic Viruses work?

A polymorphic virus is a computer virus which is capable of mutating itself when it replicates, making it more difficult to identify with antivirus software. It is a sophisticated type of virus that can wreak havoc on a computer system while avoiding detection. Polymorphic viruses can mutate their decryptors to a large number of different instances that take millions of different form.

Existing polymorphism techniques typically employ two ways of disguising code. The first rewrites the code each time so that it differs syntactically, but retains the same operational semantics. The other approach is to self-cipher; polymorphism is obtained by randomizing the order of these ciphers and using different keys.

Components of Polymorphic viruses are:

* Polymorphic Engine
* Polymorphic Encryptors
* Polymorphic Decryptors

**Metamorphic Virus**

A metamorphic virus is capable of rewriting its own code with each infection, or generation of infection, while maintaining the same functionality . Metamorphic code is code that can reprogram itself. Often, it does this by translating its own code into a temporary representation, editing this representation and rewriting itself back to normal codes.

Components of Metamorphic Viruses:

* General Obfuscation
* Entry Point Obfuscation
* Code Transposition – W32/Vundo
* Host Code Mutation
* W95 / Zmist Code Integration

## Conclusions

In summary, the report highlights the escalating threat of rapidly evolving malware to computer systems globally. Malware creators employ complex techniques to avoid detection, requiring innovative solutions. Polymorphic and metamorphic viruses employ obfuscation methods and encryption to hinder analysis. Novel malware strains like Stuxnet surpass traditional security tools, necessitating the integration of dynamic analysis and machine learning for detection. Camouflaging techniques used by malware delay detection, emphasizing the need for improved antivirus technologies. The report explores the evolution of malware camouflage and obfuscation techniques. Overall, the report underscores the ongoing challenge of combating sophisticated malware and the importance of continuous cybersecurity innovation.

## Future Works

* Gaining insight into the mechanics of ML/AI algorithms is crucial for comprehending how viruses, including metamorphic ones, can dynamically adapt in response to a computer's behavior.
* Delving into problem statements and relevant requirements within this domain is foundational, providing essential knowledge for effectively tackling cybersecurity challenges.
* Exploring cutting-edge behavioral analysis techniques is essential for enhancing the prediction and mitigation of malicious activities.
* Maintaining an ongoing assessment of the ethical considerations in this field is imperative, ensuring responsible and ethical application of knowledge and technology.

Project Supervisor

Dr Modi Chirag

Aryan Shrivastav (20CSE1005)

Aditya (20CSE1002)