Polymorphic Malware and AI in Cyber Security

Timothy Lum

CyberSecurity Service Provider Internship Program, ICS 296 & 396, Fall 2023

Advisors: Dr. Curtis Arnold, Chief Scientist – Cyber, & Dr. Robert Adamove, Sr. Associate, (Core4ce)

Problem Statement:

Technology is advancing quicker than ever and the value of data is increasing, which means that a higher priority must be placed on security. AI and machine learning are new variables in the equation that must be evaluated and understood in order to maintain the integrity of data.

Purpose:

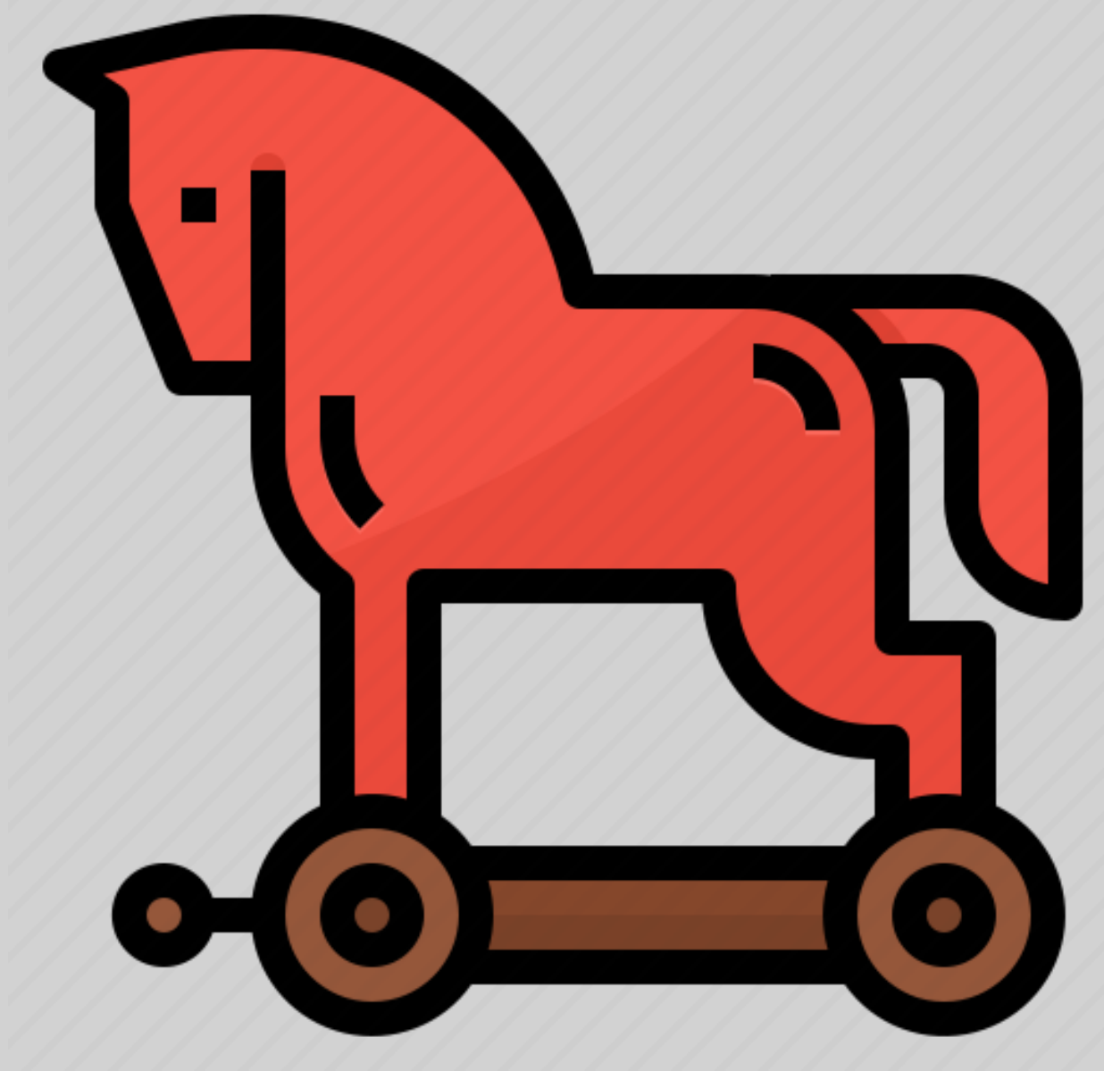
The purpose of this study is to understand how artificial intelligence and machine learning may impact the landscape of cyber security and what is required in order to prepare a strong defense against advanced unconventional cyber attacks, like polymorphic malware.

Approach:

This study utilizes secondary research with a qualitative approach on peer-reviewed academic journals and literature, along with minor use of highly credible websites for basic information. All of the literature has been published within the past 6 years.

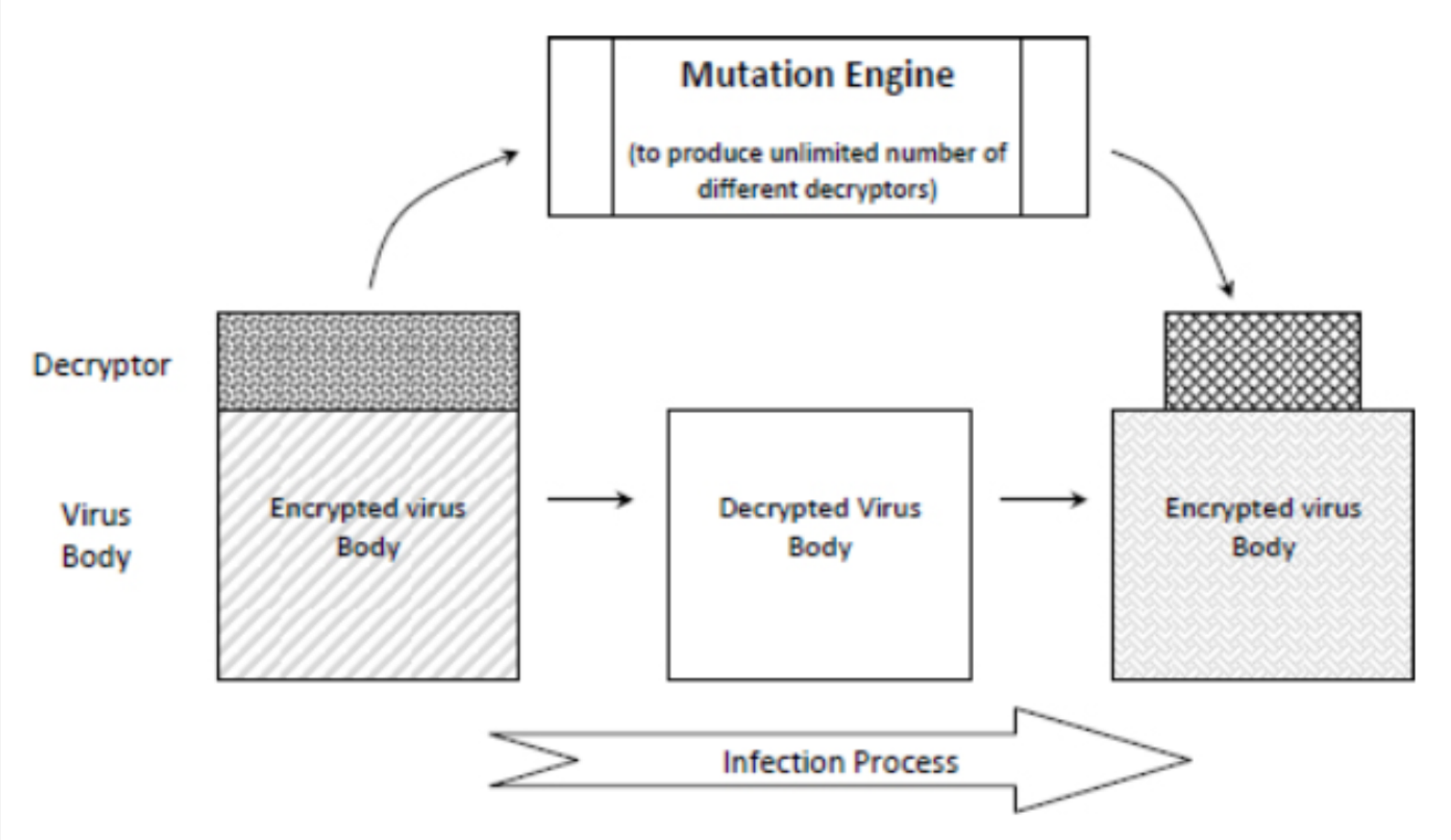
Discussion & Conclusion:

There are many different types of malware, each with a specific method of intrusion and interference. A virus is a program that will self-replicate once installed and spread from one device to another deleting files and overloading computers. Trojan Horses are a type of program that disguises as another program in order to gain access, which also includes elements of social engineering to trick individuals. Ransomware has the specific goal of taking a computers functions hostage in order to receive money to return access.



Discussion & Conclusion Continued:

In order for traditional anti-virus software to work, security products will scan for specific attributes, also known as a malwares signature. Polymorphic malware has the ability to change its code signature after every infection making it difficult to detect.



There is a variety of AI systems that also have specific methods of function. Machine learning and Artificial Neural Networks are among the most common. Utilizing artificial intelligence in cyber security has created several systems advanced enough to detect polymorphic malware. Machine learning algorithms can analyze large amounts of data and identify patterns that humans and traditional software are unable to. AI-powered malware detection can autonomously operate in real time, recognizing and responding rapidly to threats by analyzing the behavior of files, isolating the affected systems, and conducting remedial operations.
The challenges to developing AI-powered malware detection is the high start-up cost, false-positives, and potential social impact on employees. Data training and implementation can be estimated at around $500,000.

Path Forward:

Due to AI being a recent advancement and high start-up costs, there is a limited amount of quantifiable data on AI-powered malware detection. Future research recommendation is to consistently evaluate the new data that is published as trials and experiments continue.

References:

Sibanda(2023), Corbett & Sajal(2023), Moisset(2023), Scheldt(2023), Masabo(2019), Mahdavifar(2019), Berr(2017), Peterson(2017)

INFORMATION & COMPUTER SCIENCES
UNIVERSITY of HAWAIʻI at MĀNOA

UNCLASSIFIED/APPROVED FOR PUBLIC RELEASE