Chapter 5
Dealing With Polymorphic and Metamorphic Malware

Amrutha Kolhar
http://orcid.org/0009-0001-4940-3172
Karnatak University, Dharwad, India

Sridevi
http://orcid.org/0000-0002-9768-1599
Karnatak University, Dharwad, India

ABSTRACT

The evolution of malware has introduced sophisticated threats such as polymorphic and metamorphic malware, which challenge traditional cybersecurity defenses. These malware variants evade signature-based detection by dynamically altering their code through encryption, obfuscation, and self-modifying techniques. This chapter examines the characteristics and behavior of polymorphic and metamorphic malware and highlights key detection challenges, including evasion tactics like anti-sandboxing and anti-debugging. It reviews current detection and mitigation approaches, focusing on heuristic and behavioral analysis, sandboxing, and machine learning-based methods. The study also explores emerging trends in malware detection using artificial intelligence and deep learning. With the growth of immersive digital environments, the chapter discusses metaverse security concerns, identifying new attack surfaces and potential risks to virtual platforms. The findings emphasize the need for adaptive and intelligent security mechanisms to counter evolving malware threats.

DOI: 10.4018/979-8-2600-2313-6.ch005

INTRODUCTION

Malware has also developed at a very rapid rate, thus posing a significant challenge to cybersecurity, with polymorphic and metamorphic malware being the most advanced and persistent malware. In contrast to conventional malware that uses a fixed signature, which can be detected using old antivirus software, polymorphic and metamorphic malware use sophisticated means of obfuscation to avoid being detected. Polymorphic malware changes identifiable features of the malware, like encryption keys, files, or payloads, without the malicious functionality being altered. The evasion of metamorphic malware goes a step higher to ensure that every time it runs, it recodes itself, such that security systems have no idea that it is the same malware. Such malware is able to circumvent signature-based detection through these adaptive capabilities, which require more developed defensive mechanisms. Polymorphic malware typically encrypts and mutates to form new variants, whereas metamorphic malware typically rewrites code and replaces instructions in order to do so. Famous ones are the Storm Worm, which employed polymorphic technology to propagate through email, and the Simile of Metal engines, which showed how extensively it could self-modify. These threats are typically used in ransomware, banking Trojans, and advanced persistent threats (APTs), so they are considered an essential issue both to enterprises and to governments. These forms of malware are harder to detect and are harder to mitigate with the traditional signature-based strategies as opposed to more dynamic strategies. Heuristic analysis, behavioral monitoring, and machine learning have become the essential approaches in detecting malicious patterns in the case of code differences. Also, sandboxing and dynamic analysis can be used to monitor the behavior of malware in a controlled environment. But the attackers do not stand still and constantly optimize their methods, using anti-sandboxing and anti-debugging to avoid being detected. As artificial intelligence (AI) and deep learning are implemented as components of cybersecurity, combating polymorphic and metamorphic malware is increasingly becoming reliant on dynamic and real-time threat intelligence. The paper will discuss how polymorphic malware and metamorphic malware work, their development, and the issues they pose to contemporary cybersecurity. It reviews existing detection and mitigation practices and, at the same time, addresses future trends, such as AI-driven defense mechanisms and a framework of threat sharing. Knowing about these sophisticated threats, cybersecurity experts will be able to create more robust protection against the constantly evolving threat environment. The evolution of malware has a lengthy history that is closely linked to the development of earlier computer-related malware and the creation of a generic programming language (Kuriyal et al., 2022).