A Survey on Malware and Malware Detection Systems

Imtithal A. Saeed
Faculty of Computing
Universiti Teknologi Malaysia,
81310 UTM
Johor Baharu Campus, Johor,
Malaysia

Ali Selamat
Faculty of Computing
Universiti Teknologi Malaysia,
81310 UTM
Johor Baharu Campus, Johor,
Malaysia

Ali M. A. Abuagoub
College of Computer
Engineering & Sciences,
Salman bin Abdulaziz
University,
Alkharj, KSA

ABSTRACT

Over the last decades, there were lots of studies made on malware and their countermeasures. The most recent reports emphasize that the invention of malicious software is rapidly increasing. Moreover, the intensive use of networks and Internet increases the ability of the spreading and the effectiveness of this kind of software. On the other hand, researchers and manufacturers making great efforts to produce anti-malware systems with effective detection methods for better protection on computers. In this paper, a detailed review has been conducted on the current situation of malware infection and the work done to improve anti-malware or malware detection systems. Thus, it provides an up-to-date comparative reference for developers of malware detection systems.

Keywords

Malware, Malware Detection Systems, Antivirus.

1. INTRODUCTION

A more recent report from McAfee says "malware continues to grow" [1]. Thousands of new malware appear very quickly, reports from G Data and King soft Laboratory said[2, 3]. In contrast, researchers and manufacturers evolve new methods to produce improved techniques for building anti-malware [4-8]. The techniques used for creating malicious software can be categorized, in this review, into groups depending on creation and obfuscation techniques, invocation methods, platform, spreading and propagation techniques.

Malware detection system is a system used to determine whether a program has malicious intent or not [9]. Detection system includes two tasks, detection and analysis[10]. The malware detection system may or may not exist in the same system it is protecting [11]. And sometimes it's tasks divided into client and server, such as in cloud-based antivirus [8, 12]. Many improvements made on both aspects of detection and analysis [3, 10, 13-17].

In addition, technological solutions added to increase the effectiveness and the performance of malware detection systems. Such that the use of cloud computing [8], network-based detection system [18], web, virtual machine [19, 20], agent technology[21-27] or by the use of hybrid methods and technologies.

The main goal of this review paper is to investigate the current situation regarding malware and their detection systems. Moreover, the study includes analysis of the techniques and technologies used for building anti-malware.

The rest of the paper is organized as follows: Section 2 defines malware with their main. Section 3 describes the techniques used for the creation and obfuscation of malware. Section 4 discusses and compares malware classes. An extensive review of malware detection systems is presented in Section 5. Section 6 concludes the paper with remarkable comments.

2. MALWARE DEFINITION

The term malware comes from combining the two words malicious and software, and to be used to indicate any unwanted software. It was defined, generally, by G. McGraw and G. Morrisett as “any code added, changed, or removed from a software system in order to intentionally cause harm or subvert the intended function of the system” [28]. In [29] a virus has been defined as “ a generic term that encompasses Viruses, Trojans, Spywares and other intrusive code”.

Malware characterized by the ability of replication, propagation, self-execution and corruption of computer system. The corruption of computer system can affect information confidentiality, integrity and denial of services.

Replication is the important characteristics for most malware, as it ensures its existence. In some malware cases incessant replication makes exhaustion of computer resources (e.g. hard disk, RAM).

Invisibility property is used by many of malware types to evade themselves from being detected by anti-malware. It can be done by one of polymorphic or metamorphic techniques [29].

The common way for infecting a system (data or executable files, boot records of disk drives or exhausting network bandwidth) is to transfer malware from a polluted device to another uninfected one, using local or network filesystem. A malware make use of operating system vulnerabilities and software bugs, as few of software contain faults. It plants itself in to start its lifecycle at the same system or remotely controls the infection operation on another system.

3. MALWARE TECHNIQUES

For creating malware, attackers use various ways ranging from simple ordinary techniques that inserting a special piece of codes into a program file, to complex ones that use sophisticated algorithm to create obfuscated and polymorphic malware. The kind of malware produced by the ordinary techniques can be identified easily by extracting some unique characteristics to combine what called a signature.

In polymorphic malware there is variable malware in which syntaxes of mal-code mutate in each time of infection, but the semantic remain the same without change. Encryption techniques are the most common methods used in polymorphic malware.