Topic

Analysis of modern malware

Student ID – MS19813844

Name – M.D.A.I. Samaranayake

Contact # - 0773335926

Introduction

Modern malware are getting developed at a rapid rate and becoming increasingly difficult for traditional methods to detect.

This study focuses to identify methods / techniques which can be used to detect modern malware.

Problem faced

Malware which was developed only to slowdown a PC or hide a folder has become a thing of the past. Modern malware can collapse huge networks and steal huge amount of secret data within minutes of operation. The journey travelled by the malware developers were also travelled by the malware analysts. Successful analysis of a malware has resulted in effectively diffusing its operation in most of the cases. It is always a never-ending battle between malware developers and malware analysts.

To conceal the inner operation of malware, the developers use many techniques. Many of these can be broken down by effective analysis using traditional techniques. However, knowing this fact, modern malware uses stealth and split personality codings, so that the analysts will either be incapable or be slower in identifying the malware, thereby the malware itself has more time to cause its intended damage.

Proposed solution

The above-mentioned new trends require new techniques to identify and detect these modern malware. This paper attempts to review the current status of these developments and propose possible method(s)/technique(s) which can be used to detect modern malware where applicable.