MALWARE CLASSIFICATION BASED ON TARGET LOCATION

NASUHA BINTI NOOR BAHA

A thesis submitted in fulfilment of the requirements
for the award of the degree of the
Bachelor of Computer Science (Computer Systems & Networking) with Honours

FACULTY OF COMPUTER SYSTEMS & SOFTWARE ENGINEERING
UNIVERSITI MALAYSIA PAHANG

DECEMBER 2014

ABSTRACT

The combination of Malicious and Software have contribute a phrase call as Malware. Malware are software that is intended to damage or disable computers and computer systems. Malware is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. In addition malware will interrupt user on activities by using computer. The processes of classification show that malware need to classify detected objects with antivirus program. The antivirus industry used simple classification methods, comprising a unique name and the size of the detected file. However, a single antivirus could end up being called different names by different antivirus solutions, which can lead confusion. Now days, malicious programs are rapidly increases as well as the advent of new platforms of antivirus. The specific problem that malware has create, now a days there are various type of malware that become difficulty to antivirus to confirm or differentiate what type of malware attack the computer based on their characteristics. There are consists many different type or different characteristics of malware have been created. The goal of this project is to classify malware based on target class. To achieve this goal three objectives need to finish up which are to investigate system directory in window based on platform, to design malware classification system based on identified targeted class and to develop system for classifying malware based on target location. In this paper, problem had been identified and reviewed the existing malware detection. From analysis, other way had been proposed for malware classification based on target location. Output from this framework can be used by system administrator to plan and implement prevention mechanism in order to minimize future malware threat.

ABSTRAK

Gabungan perkataan virus dan perisian telah menerbitkan frasa baru iaitu Malware. Malware adalah perisian yang bertujuan untuk merosakkan atau menggangu komputer dan sistem komputer .Malware merupakan perisian yang digunakan untuk mengganggu operasi komputer, mengumpul maklumat sensitif,atau mendapat akses kepada sistem komputer peribadi. Selain malware akan mengganggu pengguna mengenai aktiviti dengan menggunakan komputer. Proses pengelasan menunjukkan bahawa malware perlu mengklasifikasikan objek dikesan dengan program antivirus. Industri antivirus digunakan kaedah klasifikasi mudah, terdiri daripada nama yang unik dan saiz fail yang dikesan. Walaubagaimanapun, satu antivirus menunjukkan boleh mengklasifikasikan malware yang sama tetapi memberi keputusan analisis yang berbeza, yang boleh membawa kekeliruan. Sehingga hari ini, malware jahat semakin pesat meningkat serta kemunculan platform baru antivirus. Masalah kepesatan jenis malware baru muncul, telah menjadi kesukaran kepada antivirus untuk mengesahkan atau membezakan jenis serangan malware komputer berdasarkan ciri-ciri mereka. Ada diantara malware baru terdiri daripada jenis yang berbeza atau ciri-ciri yang berbeza daripada malware sedia ada. Matlamat projek ini adalah untuk mengelaskan malware berdasarkan kelas sasaran di system direktori Windows. Untuk mencapai matlamat ini tiga objektif perlu selesaikan pertama mengkaji system direktori berdasakan platform Windows, kedua membentuk sistem klasifikasi malware berdasarkan kelas sasaran yang dikenal pasti dan akhir sekali untuk membangunkan sistem untuk mengklasifikasikan malware berdasarkan lokasi sasaran. Dalam kertas kerja ini, masalah telah dikenal pasti dan dikaji pengesanan malware yang sedia ada. Dari analisis, cara lain telah dicadangkan untuk pengelasan malware berdasarkan lokasi sasaran. Output daripada rangka kerja ini boleh digunakan oleh pentadbir sistem untuk merancang dan melaksanakan mekanisme pencegahan untuk mengurangkan ancaman malware masa hadapan.

TABLE OF CONTENTS

Page

CHAPTER 3 METHODOLOGY 26

CHAPTER 4 DESIGN IMPLEMENTATION 38

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

1.1 Background

The combination of Malicious and Software have contribute a phrase call as Malware. Malware are software that is intended to damage or disable computers and computer systems. Malware is software used to disrupt computer operation, gather sensitive information, or gain access to private computer systems. In addition malware will interrupt user on activities by using computer (Wikipedia). User also will feel unsecured because of malware even though an antivirus on computer or laptop. According to Mayer (2011), some computer consultants say the global malware threat has gotten so bad that conventional security measures, such as anti-virus software, are no longer adequate to fight them. It is because antivirus cannot prevent the malware 100%. Mohammad (2010) stated that "If use anti-virus, user might even be vulnerable to malware for some extent".

Computer Antivirus Researcher's Organization (CARO) (1990) had attempts to regulate the classification process of malware. The processes of classification show that malware need to classify detected objects with antivirus program. The antivirus industry used simple classification methods, comprising a unique name and the size of the detected file. However, a single antivirus could end up being called different names by different antivirus solutions, which can lead confusion. Now days, malicious programs are rapidly increases as well as the advent of new platforms of antivirus.

There are several types of malware that being classified based on their type. There are Pishing, Spyware, Trojan Horse, Virus, Worm, Adware, Crimeware, Keyloggers, Hijackers, Rogue Security Software and etc. Statistic shows that malware attack window platform 84.3 % of all virus infections can be traced back to the drive-by attacks from malicious or compromised websites according to Jonas(2013). All of these malware have different characteristics and different ways to attack computer.

1.2 Problem Statement

Hybrid malware is malicious code that combines characteristics of different types of malware (Margeret, 2008). Typically different malware have different characteristics. It is very difficult to find out exactly what types of malware have attack our computer even though with the latest antivirus. Malware give a bad threat to computer's user. The intelligence of malware now days should not be underestimated by computer's user. It should be a main reason why user should secure their computer from the malware. It is because the malware are created with different characteristic to create a problem to computer's user.

The specific problem that malware has create, now a days there are various type of malware that become difficulty to antivirus to confirm or differentiate what type of malware attack the computer based on their characteristics. There are consists many different type or different characteristics of malware have been created. According to Michael (2007), numerous attacks, such as worms, phishing, or other malware will threaten the privacy of users. A core element of defense against these attacks is anti-virus. But sometimes an antivirus are usually difficult to classified or find out what is the type of malware had attack the computer, it show that different antiviruses give a different result of type of malware attack the computer.

It clearly shows that an antivirus difficult to identify type of malware based on characteristics. There are many characteristics that sometime an antivirus difficult or confuse to characterize the type of malware. Different antivirus gives different type of malware even though it is the same malware actually.

1.3 **Goal and Objectives**

The goal of this project is to classify malware based on target class. To achieve this goal three objectives need to finish up which are:

i. To investigate system directory in window based on platform
ii. To design malware classification system based on identified targeted class.
iii. To develop system for classifying malware based on target location.

1.4 Scope Project

1.4.1 Functionality

This project is about to classify malware by using target location on Window directory system. Window will be used as a platform. Based on the classification target class of malware it will attack based on location which are application, data, system and Disk Operating System (DOS).

1.4.2 Type of System

System that will be generated can classify the malware by using their target location. System will show that malware attack window on system directory, therefore it is important type of system directory on Window and we can classify based on malware target location.

1.5 Methodology

Based on Figure 1.1, it shows that to accomplish or achieve the goal and three objectives of this project which is malware classification using target location. There are seven steps need to complete, which is:

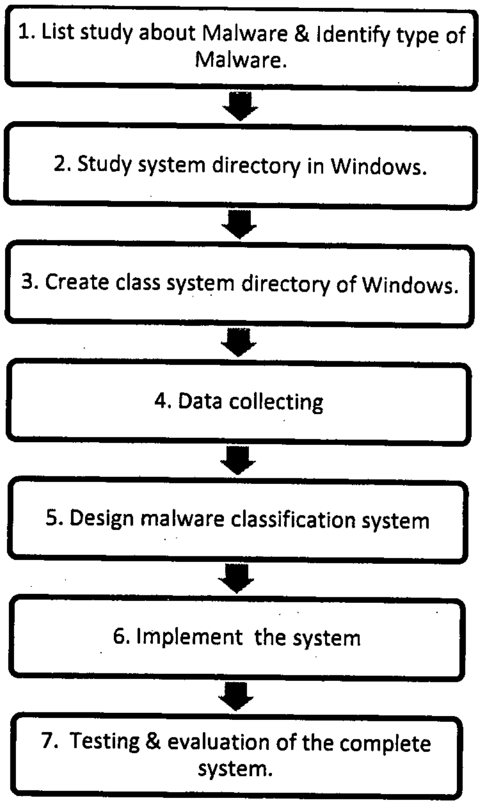
1. List study about Malware & Identify type of Malware.
2. Study system directory in Windows.
3. Create class system directory of Windows.
4. Data collecting
5. Design malware classification system
6. Implement the system
7. Testing & evaluation of the complete system.

Figure1.1 Methodology of project

First objective which is to investigate system directory in Window based on platform will be achieved after completed step 2. From Figure 1.1, Step 2 is to study system directory in Window. It is important to fully understand the type of system directory in Window, whether it is application, data, system or Disk Operating System (DOS). It is because this project is about malware classification using target location. Therefore step 1 also very important which is to study about Malware and identify type of Malware. After completing and understanding step 1 and step 2 first objectives will be achieve.

Second objective to design malware classification system based on identified targeted class. Before objective two will be achieve, there are several steps need to complete. From Figure 1.1,step 3 until step 6 which is from create class system directory of Windows until implement the system for classification of malware using target location will be complete to achieve second objective. System will be implementing by using Visual Basic Express 2008

Thirdly, after implementing the system of malware classification using target location on Window step 7 on Figure 1.1 which is testing and evaluating the complete system. It is necessary because testing is to ensure the complete system does not have problem and it can be used. Therefore third objective to develop system for classifying malware based on target location will be completed. Finally, the main goal of this project to classify malware based on target class will be achieved.

CHAPTER 2

LITERATURE REVIEW

2.1 Overview

In this chapter, there will be five subtopics that will cover from the definitions of the Malware Classification Based on The Malware Target Location.

Subtopic 2.1 will describe the definition and structure of malware and history of malware. Subtopic 2.2 will define and discuss about all the malware type. Subtopic 2.3 will explain about malware target. Subtopic 2.4 will cover on the comparison of others research about malware classification. The last subtopic 2.6 will discuss in detail about the software requirements in developing the applications in this project.

Overall contents in this chapter will provide reader with the detail information of the method implementation that will be carried out in this project.

2.2 Malware

From the study, Malware is any kind of unwanted software that is installed without user not knowing and unwillingness. Viruses, worms, and Trojan horses are examples of malicious software that are often grouped together and referred to as malware. But now a day there are some several type of malware have been released to interrupt computer user. Even though user have being careful from one of the computer crime there are still many way to spread this malware. For example from the webpage user being opened, this is called as cybercriminals. Cybercriminals sometimes try to trick you into downloading rogue (fake) security software that claims to protect you against malware. This rogue security software might ask you to pay for a fake product, install malware on your computer, or steal your personal information (safety n security of software, Microsoft, (2014).

In addition, according to Jolla (2014), user should know there are many ways malware can be spread such as from peer to peer programs which is from the university network. Malware also can be able from the downloaded from other programs, file, and also email attachment. Student which always find the material of study always being lacked of the security of their computer, they should beware of the webpage which is sometimes consists of malware. After their computers have been attack by malware, it can disturb windows system. There are several signs computer user should know that their computer infected by the malware which is there will be pop-ups that run advertising, if suddenly screen turns black and all start menu items and sometimes desktop icons disappear in a blink of eye and also computer running very slowly than usual, it shows that computer have be run other programs in the background that cannot being seen on the interface.

Malware have being introduced since a long time ago which is in the era computer have being introduced. From the study, the history of malware has started since in the era of 1940. Based on GDATA and LAVASOFT, on 1949, the theoretical preliminary works on computer viruses by John von Neumann (1903-1957) develop the automatons. Automaton is developing of method which is can describe and analyzing discrete of system. In addition, according to Amal (2004) **Automatons** are abstract models of machines that perform computations on an input by moving through a series of states or configurations. On 1971, computer virus which is CREEPER have been develop and infected computer on ARPANET. On 1981, Adleman employs the term "computer virus" for the first time in conversation with Fred Cohen. First computer virus for MS-DOS known as 'Brain' was released in January 1986. It can be affected the boot sector of storage media formatted in the FAT file system written by two brothers from Pakistan, Basit and Amjad.

On 1987, stoned is computer virus written from Wellington's university. After the first Macintosh viruses have surfaced in the form of nVir and Peace, Apple decided to load the virus search program Virus-Rx on every computer. The so-called "Cascade-Virus" is the first encrypted virus. This causes, for the first time in Germany, the letters on a page to slide downwards where they collect in a little heap. The files were destroyed. The first virus for Amiga (SCA) infects the boot sector and displays a message from time to time. In December, a well-meaning American student crippled e-mail communication and networks worldwide with the first computer worm. The "Christmas tree" worm draws a Christmas tree on the screen while in the background, it sends itself to all the e-mail addresses it can find on the system.

Figure 2.1 show the growth and evolution of malware according to ESET (2010) there are million number of malware samples had being found and classified as unique or comes out from different sample. Nowadays development of malware had being clarified as a profitable sources product. The developer will use the malware to spam, steal an information. Based on the analysis of Panda (2010) new malware keep on increasing frpm time to time and this phenomena had attract the serious concern from the security group around the world. For example Panda Security Lab reported that one third existing computer malware are created in between January to October 2010.

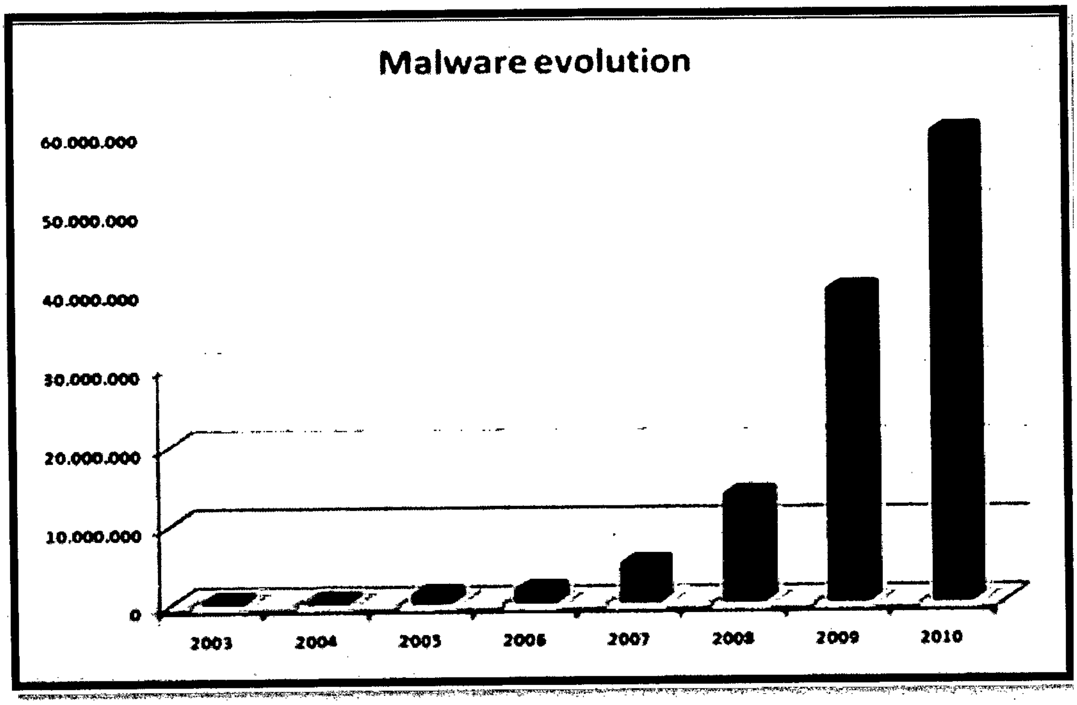

Figure 2.1 Show Malware Evolution from 2003 to 2010

The contributions of other types of malware are continuously happen until this era. It shows that malware are computer crime that cannot be stopped but only to prepare the computer with the high of security to prevent from the malware. There are several types of antivirus has be develop, user has the right to choose whether they want secure their property which is computer and all data or file in computer or let the malware attack their computer. Lastly, an antivirus can only prevent an attack from the malware not to stop the attack.

2.3 Malware Types

Malware is a computer program that many adverse impact on the computer. The effects can be seen on a computer screen or latent some of them cannot be seen on the computer screen. In others word can corrupt data in the computer and disturb the performance of the computer itself. Malware creation had given negative impact to user which is early it being created for an experiment on computer and do pranks such on email. But it has lure to vandalism and destruction to computer. Now a day, malware are created for make a profit through forced advertising, stealing user information and email spam. There are many types of malware that have been disturbing the computer. Figure 2.2 shows the example of malwares which are Trojan, Spyware, Pishing, Virus, Worm, Adware, Rootkit, Keylogger, Crimeware, Bot, Bug, Ransomware, and Hijackers.

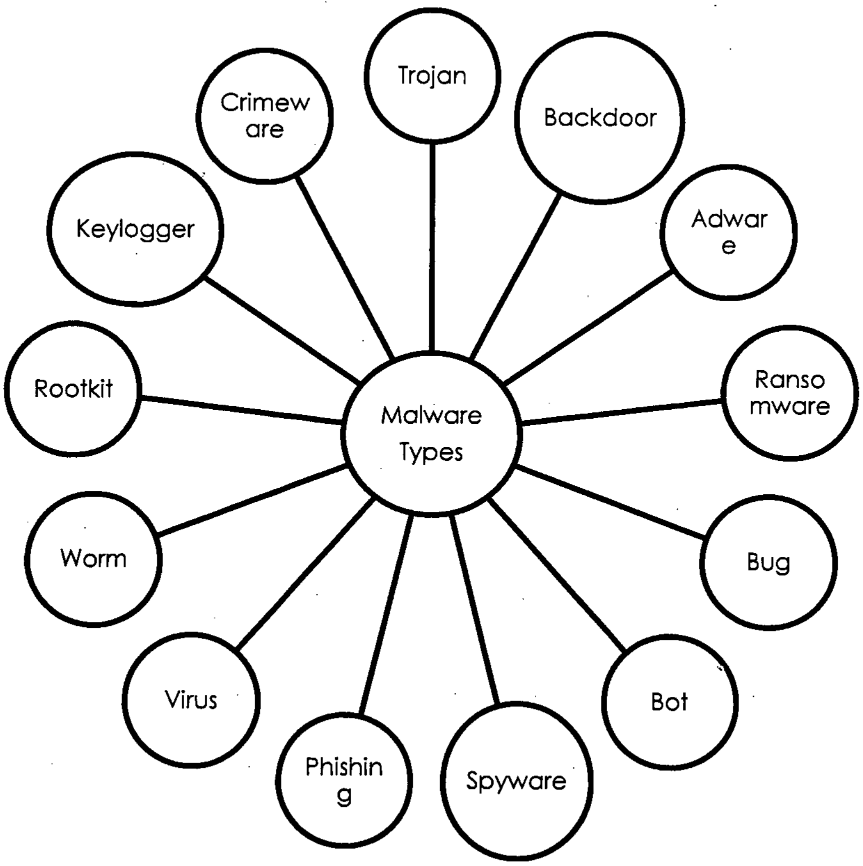

Figure 2.2 Types of Malware Attack Network and Computer.

Trojan horse or the shortened name is Trojan. Trojan is one type of malware that user can see as normal file or normal program, but actually Trojan only disguise as a normal file. It is very dangerous because it can trick users downloading and installing a dangerous malware accidentally. Trojan can give an access to malicious party until it give a bad infection to computer. In addition, after the attacker has found à way to access to computer, it is high possibility for the attacker to steal data by logins without unauthorized, steal a financial data of user since user open financial website on the computer. Trojan also have an ability install more malware, modify data on the computer and even though Trojan can also monitor user activity.

Adware is short for advertising-supported software. It is a type of malware that automatically give or update an advertisement to user without asking first. It is usually display unwanted advertisement the software that user have been downloaded previously. It is because the authors of the software want to recover development process by do free advertisement. Adware is dangerous because it is designed to collect data from the website that user visits and send back the collected data to the company and deliver advertising without permission from user. It clearly shows that advertisement from Adware may be seen as an annoyance, a distraction, or an invasion of privacy to the user.

Bot is derived from the word robot and is an automated process that interacts with other network services. Bots often automate tasks and provide information or services that would otherwise be conducted by a human being. A typical use of bots is to gather information, or other web interfaces. With a botnet, attackers can launch broad-based, remote-control, flood-type attacks against their target. In addition to the worm-like ability to self-propagate, bots can include the ability to log keystrokes, gather passwords, capture and analyze packets, gather financial information, launch DOS attacks, relay spam, and open back doors on the infected host. Bots have all the advantages of worms, but are generally much more versatile in their infection vector, and are often modified within hours of publication of a new exploit (CISCO).

Bug is a latent malware that will take a long time before user discover the existence. In the context of software, a bug is a flaw produces an undesired outcome (Nate Lord, 2012). This type of malware usually disturb in the source code or compiler of program in the computer. It will harm a program's behavior and cause crashing or freezing significantly. Bug is present in many forms in the computer software. For example security bug are the most severe type of bugs, it can allow attackers to access or bypass user authentication, it also can override the access of the privilege even though still data of user.

According to Konrad Krawczyk (2014), Ransomware is type of malware that leaves de-cryption key on victim's PC. It shows that this type of malware will disturb user's file by locks down the file and it forced user to find out a way to regain access to their data. One piece of Ransomware, dubbed CryptoDefense, not only encrypts a victim's files, but also leaves the decryption key on the same PC as well. This type of malware also display a message that force user to pay the malware creator to remove the restriction and regain access to their computer. Ransomware spread like a worm end up in the computer by downloaded file through a network.

Rootkit is type of malicious software that are designed to remotely access or control the computer without user know even though the security program not alert to it. Once the rootkit have been installed the malicious party will remote execute files, access the information, steal the information and also can modify the system. It is also can disturb the security software with alter the software that could detect the rootkit. According to Nate Lord (2012), rootkit prevention, detection, and removal can be difficult due to their stealthy operation. It is because are hides or latent even though security program difficult to detect them. User can protect from rootkit by regularly patching vulnerabilities in software, application, and operating system, updating virus definitions, and also avoiding suspicious downloads (veracode, 2012).

Spyware is type of malware that are installed in computer without the knowledge by user to spying user activity on computer. In order to do spying, spyware also have function collect user private information such as account information, logins and also financial data. Spyware also have an ability modifying security software or browsers to interfere network connections (veracode, 2012). In addition, spyware is installed when a user installs a piece of free software that they actually wanted. When the desired software is installed, the spyware will piggyback on the installation and start collecting data from the user's activities. The user can also be tricked into installing the spyware through a Trojan horse as well as it pretending to be a free piece of security software.

Common malware that always be heard is virus. It has the capability to copying itself and spread itself to other computers. Viruses often spread to other computer when user attaching various program. It can execute the code of program when user launches the infected program into their computer. Furthermore, viruses also can spread through script files, document and cross-site scripting vulnerabilities in web applications (veracode, 2012). In addition virus also can be used to steal information, harm computer host even though steal money.

The most common type of malware is Worms. According to Bradley, computer worms are malicious software applications designed to spread via computer networks. Computer worms are one form of malware along with viruses and Trojans. A person typically installs worms by inadvertently opening an email attachment or message that contains executable scripts. Once worm in computer it spontaneously generate additional email messages contain copy of worm. Worm also can disturb on TCP ports to allow for other unauthorized applications.in addition it also can make the LAN flood with DOS data transmissions (Wireless/Networking, 2014). There are several characteristics that user can distinguish worms other than viruses. A major differences is it have an ability to replicate itself and spread independently while other viruses rely on human activity to spread.

Phishing is an attempt by a hacker to obtain confidential information about user. For example user will receive an email from some company that will ask about their detail information. The sources of an email look like from a trusted company and also contain convincing information but in reality hackers have created a fake email to obtain the information especially about financial information. Sometimes users only click the link that they received from email just enough to install the malware on computer. Phishing messages usually take form of fake notification from banks, providers and other organizations.

Generally, various factors can make computers more vulnerable to malware attacks, including defects in the operating system design, having all of the computers on a network run the same OS, giving users too much permissions or just using the Windows OS due to its popularity, it gets the most malware written for it. The best protection from malware continues to be the usual advice and be careful about what email attachments user try to open, be cautious when surfing and stay away from suspicious websites, and install and maintain an updated, quality antivirus program. Even though user had installed an antivirus, it cannot stop the attacks of all the malware 100% just can prevent it.

Table 2.1 shows the comparison different type of malware according to their distribution ways and also the way of malware attack in system directory. Table shows that some of the malware such as worm and ransomware had same way to distribute or spread into system directory. An antivirus can get confused to classify them based on their distribution or characteristics.

Table 2.1 Types of malware, way it distribute and way it attack to computer.

No	Types	Way to Distribute	Way to Attack
1.	Trojan	➢ Accidentally user downloading or installing from the website	➢ Give unauthorized access to malicious party to computer. ➢ Attacker can access data to computer & steal data of user such as financial data.
2.	Adware	➢ Feed up user with undesired and pop ups or redirect to unwanted pages.	➢ Can hijack to homepage and force user to visit webpage. ➢ allow pop up advertisement ➢ Cause slowdowns and software conflicts which can make computer unstable.