LAB 1

Malware Overview

By the end of this section of the practical, you should be able to:

- Define what malware is.
- Classified the different type of malware
- Describe the characteristic, behavior and the impact of the malware

1.1 Introduction

Malware is define as Malicious or malevolent software and it is used by cybercriminals, hacktivists and nation states to disrupt computer operations, steal personal or professional data, bypass access controls and otherwise cause harm to the host system. Appearing in the form of executable code, scripts, active content or other software variants, there are many different classes of malware which possess varying means of infecting machines and propagating themselves.

Malware author write thousands of new malicious software daily, it can be newly written malicious code or modified from existing malicious code available from the Internet. The reasons why the malicious code is written can be different, it can be simply because the author wanted to publicize its hacking ability, or to see how severe their programs can wreak a server, or want to get a special message out, or disrupt operations or gather private information. In a more serious matter malware can also steal credential information such as Social Security numbers, credit card information, email addresses and passwords for the purpose of identity thieves.

Certain malware applications hide behind legitimate applications disguise themselves as important application or even fake antivirus applications. Some malware also have the ability to capture every keystroke the machine user types on their keyboard, acting as keystroke logger. Through this features the hackers behind the malware can pick out the user password, login ID and other credential information. In general a malware infection can cause the user machine to:-

- Disrupts operations.
- Steals sensitive information.
- Allows unauthorized access to system resources.
- Slows computer or web browser speeds.
- Creates problems connecting to networks.

1.2 Classification of Malware

Malware can be classified as:-

Viruses

Computer program that is usually hidden within another seemingly innocuous program and that produces copies of itself and inserts them into other programs and usually performs a malicious action (as destroying data)

Worms

usually small self-contained and self-replicating computer program that invades computers on a network and usually performs a destructive action

Trojans Horse

A seemingly useful computer program that contains concealed instructions which when activated perform an illicit or malicious action (as destroying data files)

Spyware

Software that is installed in a computer without the user’s knowledge and transmits information about the user’s computer activities over the Internet Adware – software installed that provides advertisers with information about the users browsing habits, thus allowing the advertiser to provide targeted ads.

Backdoors

Bypasses normal security controls to give an attacker unauthorized access.

Rootkits

Trojan horse backdoor tools that modify existing operating system software so that an attack can keep access to and hide on a machine

Botnet

Bots are software programs created to automatically perform specific operations. While some bots are created for relatively harmless purposes (video gaming, internet auctions, online contests, etc), it is becoming increasingly common to see bots being used maliciously. Bots can be used in botnets (collections of computers to be controlled by third parties) for DDoS attacks, as spambots that render advertisements on websites, as web spiders that scrape server data, and for distributing malware disguised as popular search items on download sites.

Task 1

Malware Case Study

In a group discuss the type of malware and find at least 4 recent malware for EACH of the malware types. The discussion should cover:-

1. The year the malware is released.
2. The platform the malware is targeting (Mac OS, Windows, Linux, Android, IOS and etc)
3. How the malware infect the host/ target?
4. What is the vulnerability that the malware exploit?
5. The impact of the malware to the host.
6. The step to remove the malware.

Write a simple report for this task. The report should mention the source of the information that you refer.