Types of Computer Malware: Explained

Published on Wednesday, May 17, 2017

Introduction

Malware stands for “Malicious Software”. It performs unwanted tasks. It may cause serious damage or invasion to our computer. Stealing data, stealing the password, infecting the computer are the examples of Malware programs. Even a pop-up advertising is a malware program.

“Ransomware” is in news these days and is malicious software that blocks access to the computer until money is paid.

Types of Malware

I. Virus (Vital information resource under seize): It is a computer program that spreads from one computer to another and it causes serious damage or harm to the computer system by deleting files, by deleting everything on the hard disk etc. The purpose of this program is to disrupt the operation of a computer system. It can even utilise an e-mail program to spread the virus to another computer.

II. Trojan Horse: It is not a virus. It is a computer program that seems to be a game but in reality, it damages the computer system once you run it. It may even erase the hard disk.

III. Worm: It is a type of software that makes use of security holes and computer network in order to replicate itself. It scans the network for machines that carry a security hole and then it copies itself there and starts replicating. Examples: Code Red, Mydoom, Brontok.

IV. Spyware: It is a malware installed on the computer systems that collects information about users without their knowledge. It can be used for other purpose of secretly monitoring users in firm, corporate. Collection of information includes visited websites, IP address, browser history etc. Examples of spyware are Click-Jacker, Key-logger.

V. Adware: The ads that automatically appear on our screen when we connect to the internet are displayed by financially supported software called Adware.

VI. Browser Hijacking Software: It is an advertising program that modifies our browser settings, displays pop-up advertisements and creates desktop shortcuts.

Some points regarding cyber crime

I. Cyberstalking: The use of internet or other electronic means to harass or stalk a group, an organisation or an individual. It is done in real time or even in offline

mode.

II. Identity theft: It is an unauthorised access to someone's identity or personal information to get financial benefits or any other benefits without the consent of that individual.

III. Phishing: It is a fraudulent practice of getting someone's personal information such as login credentials, cards numbers etc through email.

IV. Eavesdropping: It is secretly listening or accessing someone's phone calls, instant messages, video conference or fax transmission.