COMPUTER SECURITY THREATS

Malware: **Malware**, short for **malicious software**, consists of programming (code, scripts, active content, and other software) designed to disrupt or deny operation, gather information that leads to loss of privacy or exploitation, gain unauthorized access to system resources, and other abusive behavior. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code. Software is considered to be malware based on the perceived intent of the creator rather than any particular features. Malware includes **computer viruses**, **worms**, **trojan horses**, **spyware**, **dishonest adware**, **scareware**, **crimeware**, most **rootkits**, and other malicious and unwanted software or program. In law, malware is sometimes known as a **computer contaminant**. Some examples of malware are **Melissa Virus, David Virus, Cabir, Code Red worm, Ramen worm.**

Computer Virus: A **computer virus** is a computer program that can copy itself and infect a computer. A true virus can spread from one computer to another (in some form of executable code) when its host is taken to the target computer; for instance because a user sent it over a network or the Internet, or carried it on a removable medium such as a floppy disk, CD, DVD, or USB drive. Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer. The first PC virus in the wild was a boot sector virus dubbed **Brain**, created in 1986 by the **Farooq Alvi** Brothers in Lahore, Pakistan. Some more examples of viruses are **Elk Cloner, Chernobyl Virus, and CIH Virus.**

Worm: A **computer worm** is a self-replicating malware computer program, which uses a computer network to send copies of itself to other nodes (computers on the network) and it may do so without any user intervention. This is due to security shortcomings on the target computer. Unlike a computer virus, it does not need to attach itself to an existing program. Worms almost always cause at least some harm to the network, even if only by consuming bandwidth, whereas viruses almost always corrupt or modify files on a targeted computer. Some examples of worms are **Morris worm, My doom, ExploreZip.**

Adware: **Adware**, or **advertising-supported software**, is any software package which automatically plays, displays, or downloads advertisements to a computer. These advertisements can be in the form of a pop-up. They may also be in the user interface of the software or on a screen presented to the user during the installation process. The object of the Adware is to generate revenue for its author. Adware, by itself, is harmless; however, some adware may come with integrated spyware such as keyloggers and other privacy-invasive software. Examples are **Ask.com Toolbar, Bonzi Buddy, ClipGenie, Comet Cursor, Cydoor, DollarRevenue, FlashGet, Gator, Mirar Toolbar, MyWay Searchbar, Spotify, Tribal Fusion, Viewpoint Media Player, WhenU SaveNow, Zango products.**

Spyware: **Spyware** is a type of malware that can be installed on computers, and which collects small pieces of information about users without their knowledge. The presence of spyware is typically hidden from the user, and can be difficult to detect. Typically, spyware is secretly installed on the user's personal computer. Sometimes, however, spywares such as keyloggers are installed by the owner of a shared, corporate, or public computer on purpose in order to secretly monitor other users. Spyware is known to change computer settings, resulting in slow connection speeds, different home pages, and/or loss of Internet connection or functionality of other programs. Some examples are **Gator, BargainBuddy.**

Spamware: **Spamware** is software designed by or for spammers. Spamware varies widely, but may include the ability to import thousands of addresses, to generate random addresses, to insert fraudulent headers into messages, to use dozens or hundreds of mail servers simultaneously. The sale of spamware is illegal in eight U.S. states. Another type of spamware is software used to search for e-mail addresses to build lists of e-mail addresses to be used either for spamming directly or to be sold to spammers.

Email spams: **Email spam**, also known as **junk email** or **unsolicited bulk email** (**UBE**), is a subset of spam that involves nearly identical messages sent to numerous recipients by email. Definitions of spam usually include the aspects that email is unsolicited and sent in bulk. One subset of UBE is *UCE* (unsolicited commercial email). The opposite of "spam," email which one wants, is called "ham".

Trojan horse: A **Trojan horse**, or **Trojan**, is a destructive program that masquerades (give dodge) as an application. The software initially appears to perform a desirable function for the user prior to installation and/or execution, but

(perhaps in addition to the expected function) steals information or harms the system. Unlike viruses or worms, Trojan horses do not replicate themselves, but they can be just as destructive. Some example of Trojan horse is **Slavebot**.

Hacker: A **hacker** is a person who breaks into computers and computer networks for profit, in protest, or because they are motivated by the challenge. The term hacker is reclaimed by computer programmers who argue that someone breaking into computers is better called a **cracker**, not making a difference between computer criminals ("black hats") and computer security experts ("white hats"). Some white hat hackers claim that they also deserve the title hacker, and that only black hats should be called crackers.

Hacking can be beneficial: Since a large number of hackers are self taught wonders, some corporations actually employ computer hackers as part of their technical support staff. These individuals use their skills to find flaws in the company's security systems so that they can be repaired quickly. In many cases, this type of computer hacking helps prevent identity theft and other serious computer related crimes.

Means through which Viruses, Worms and Adware spreads:

1. Infected flash drives or floppy disks.
2. E-mail attachments.
3. Surfing insecure websites.
4. Installing pirated softwares.

How virus can spread through flash drive?

Use of flash memory and floppy disk is quite insecure for the health of a computer. Suppose you do not have a virus on your computer and you are copying data from any other computer with the help of flash memory of floppy disk, you may copying the infected data. If the antivirus is not installed on your computer then the virus creeps in silently into your computer and works as cancer.

Protection: Always keep antivirus installed on your computer and update it regularly. When you plug in flash memory or insert floppy disk into your computer get it scanned for viruses at first hand and then make use of it.

How email spreads virus?

Email messages with a file attachment are the major cause of spreading viruses. If you get the email with attachment never tries to open it unless you are sure about its source of delivery. You can identify the email having an attachment with a paper clip icon next to the email in your inbox.

Insecure websites are also the cause of spreading virus:

There are some web sites that are not protected and secure to surf, when we open such web sites there are ads or some other stuff that can allure us and we click on that, by doing so virus shifted from that website to our computer.

Protection: Always keep antivirus installed on your computer and update it regularly. Turn on its real time protection mode so that it always search files from internet for viruses as they enter into your computer.

Pirated soft wares are also the cause of spreading virus: