Malware

Computer Virus is a program that infects some executable software of the computer and causes that software, when run, to spread the virus to other executable software. The virus may also contain a payload which performs other actions, often malicious. A **Computer worm** is the program which actively transmits itself over a network to infect other computers. It too may carry a payload. The difference between the virus and worm is that the virus requires user intervention to spread, whereas a worm spreads automatically. Infections transmitted by email or Microsoft Word documents, which depends on the recipient opening a file or email to infect the system, can be called as viruses rather than worms.

The first network-borne infectious programs, originated in multitasking Unix systems. The first well-known worm was the Internet Worm of 1988, which infected SunOS and VAX BSD systems. It exploited the security holes in the network server programs and started itself running as a separate process.

Some important Malicious Programmes are:

Trojan horses

Trojan horse is any program that invites the user to run it, concealing a harmful or malicious payload. The payload may take effect immediately and can lead to many undesirable effects, such as deleting the user's files or further installing malicious or undesirable software. Trojan horses known as droppers are used to start off a worm outbreak, by injecting the worm into users' local networks. When the user installs the software, the spyware is installed alongside.

Root kits

Root kits are programmes that modify the operating system of the computer while the malware remains concealed. Once a malicious program is installed on a system, it is essential that it stay concealed, to avoid detection and disinfection. Techniques known as root kits allow this concealment, by modifying the host operating system so that the malware is hidden from the user.

Backdoors

It is the method of bypassing normal authentication procedures. Once a system has been compromised, one or more backdoors may be installed. Backdoors may also be installed prior to malicious software, to allow attackers entry. Crackers typically use backdoors to secure remote access to a computer, while remaining hidden from casual inspection. Crackers generally use Trojan horses, worms, or other similar programmes to install the Backdoor.

Spyware programs

These are programmes commercially produced for the purpose of gathering information about computer users, showing them pop-up ads, or altering web-browser behavior for the financial benefit of the spyware creator. For example, some spyware programs redirect search engine results to paid advertisements. Spyware programs are sometimes installed as Trojan horses of one sort or another.

Botnets.

Botnet is the malware used to coordinate the functioning of many infected computers at the same time. The Botnet, logs in to an Internet Relay Chat channel or other chat system. The attacker can then give instructions to all the infected systems simultaneously. Botnets can also be used to push upgraded malware to the infected systems, keeping them resistant to anti-virus software or other security measures.

Nonresident viruses

Nonresident viruses can have a finder module and a replication module. The finder module is responsible for finding new files to infect. For each new executable file the finder module encounters, it calls the replication module to infect that file.

Resident viruses

Resident viruses contain a replication module that is similar to the one that is used by the nonresident viruses. This module, however, is not called by a finder module. The virus loads the replication module into memory when it is executed instead and ensures that this module is executed each time the operating system is called to perform a certain operation.

A computer virus hoax

It is a message warning the recipient of a non-existent computer virus threat. The message is usually a chain e-mail that tells the recipient to forward it to everyone they know.

Data-stealing malware

Data-stealing malware is a web threat that steals the personal and proprietary information. Typical examples of Data stealing programmes are key loggers, screen scrapers, spyware, adware, backdoors, bots etc. Some important data stealing programmes are:

1. **Bancos**. It is an info stealer that waits for the user to access banking websites then spoofs pages of the bank website to steal sensitive information.

2. **Gator**. It is the spyware that covertly monitors web-surfing habits, uploads data to a server for analysis then serves targeted pop-up ads.

3. **LegMir**. It is the spyware that steals personal information such as account names and passwords related to online games

4. **Qhost.It** is the Trojan that modifies the Hosts file to point to a different DNS server when banking sites are accessed then opens a spoofed login page to steal login credentials for those financial institutions.

Multipartite virus

It is a form of computer virus that infects and spreads in multiple ways. The term Multiple Virus was coined to describe the first viruses that included DOS executable files and PC BIOS boot sector virus code.

Computer Spams

The word Spam is used to describe the abuse of electronic messaging systems to send unsolicited bulk messages indiscriminately. The most widely recognized form of spam is e-mail spam. Different forms of Spams are:

1. E-mail spam

Email Spam is also known as Unsolicited Bulk Email or UBE or Junk mail, or Unsolicited Commercial Email (UCE).It the is the practice of sending unwanted e-mail messages, frequently with commercial content, in large quantities to an indiscriminate set of recipients.

2. Mobile phone spam - SpaSMS

Mobile Spam is also known as SpaSMS. Mobile phone spam aims at the text messaging service of a mobile phone. This can be especially irritating to customers not only for the inconvenience but also because of the fee they may be charged per text message received in some markets.

3. Instant Messaging Spam- Spim

Instant Messaging spam, also known as Spim, makes use of instant messaging systems. Although less ubiquitous than its e-mail counterpart, Spim is reaching more users all the time. One way to protect against Spim is to only allow messages from people on your friends lists.

Online game messaging spam

Many online games allow players to contact each other via player-to-player messaging, chat rooms, or public discussion areas. This may create Spams.

Mobile Phone Virus

A mobile phone virus is an electronic virus that targets mobile phones or wireless-enabled PDAs. Common forms of mobile viruses include

1. Cabir.It Infects mobile phones running on Symbian OS. When a phone is infected, the message **'Caribe'** is displayed on the phone's display and is displayed every time the phone is turned on. The worm then attempts to spread to other phones in the area using wireless Bluetooth signals.

2. Duts: It is a form of parasitic file infector virus and is the first known virus for the PocketPC platform. It attempts to infect all EXE files in the current directory.

3. Skulls: It is a Trojan horse piece of code. Once downloaded, the Skulls, replaces all phone desktop icons with images of a skull. It also will render all phone applications, including SMS and MMS services.

4. Commwarrior: It is the first worm to use MMS messages in order to spread to other devices. It can spread through Bluetooth and infects devices running under OS Symbian Series 60. The executable worm file once launched hunts for accessible Bluetooth devices and sends the infected files under a random name to various devices.

How computers become Non Immune?

Various factors make a computer system more vulnerable to malware. Some of them are :

1. **Homogeneity** – When all computers in a network run the same OS, if you can exploit that OS, you can break into any computer running it.
2. **Defects** – Malware leveraging defects in the OS design.
3. **Unconfirmed code** – Codes from a floppy disk, CD-ROM or USB device may be executed without the user's agreement.
4. **Over-privileged users** – Some systems allow all users to modify their internal structures.
5. **Over-privileged code** – Most popular systems allow code executed by a user all rights of that user.

Protect your PC and Mobile phone

Many users install anti-virus software that can detect and eliminate known viruses after the computer downloads or runs the executable. There are two common methods that an anti-virus software application uses to detect viruses.

1. The most common method of virus detection is, using a list of virus signature definitions. This works by examining the content of the computer's memory, its RAM, and boot sectors and the files stored on fixed or removable drives like hard drives, floppy drives etc, and comparing those files against a database of known virus "signatures
2. The second method is to use a heuristic algorithm to find viruses based on common behaviors. This method has the ability to detect viruses that anti-virus security firms have yet to create a signature for.

On-access scanning

Some anti-virus programs are able to scan opened files in addition to sent and received e-mails 'on the fly' in a similar manner. This practice is known as "on-access scanning." Anti-virus software does not change the underlying capability of host software to transmit viruses. Users must update their software regularly to patch security holes. Anti-virus software also needs to be regularly updated in order to prevent the latest threats.

Maintain Backup data

If a backup session on optical media like CD and DVD is closed, it becomes read-only and can no longer be affected by a virus so long as a virus or infected file was not copied onto the CD. Likewise, an operating system on a bootable CD can be used to start the computer if the installed operating systems become unusable. Backups on removable media must be carefully inspected before restoration. The **Gammima virus**, for example, propagates via removable flash drives.

Another method is to use different operating systems on different file systems. A virus is not likely to affect both. Data backups can also be put on different file systems.

Recovery methods

Once a computer has been infected by a virus, it is usually unsafe to continue using the same computer without completely reinstalling the operating system. There are a number of recovery options that exist to remove the virus. These options depend on severity of the type of virus.

Virus removal

System Restore tool

The System Restore too restores the registry and critical system files to a previous checkpoint’

This can be done in Windows Me, Windows XP and Windows Vista etc. Often a virus will cause a system to hang, and a subsequent hard reboot will render a system restore point from the same day corrupt. Restore points from previous days should work provided the virus is not designed to corrupt the restore files or also exists in previous restore points. Some viruses like **CiaDoor** disable the system restore and other important tools such as Task Manager and Command Prompt. The virus modifies the registry to do the same, except, when the

Administrator is controlling the computer, it blocks all users from accessing the tools.

Reinstallation

Reinstalling the operating system is another approach to virus removal. It involves simply reformatting the OS partition and installing the OS from its original media, or imaging the partition with a clean backup image.

D.Mohankumar