Comparison of The Computer Viruses from Time to Time

Feri Sulianta,

DOI: https://doi.org/10.37178/ca-c.23.1.139

***Feri Sulianta**, Widyatama University*
Email: feri.sulianta@widyatama.ac.id

Abstract

The term Virus was first published academically by Fred Cohen in 1984 in a scientific paper. Computer viruses have a way of working identical to biological viruses in general, so it's no wonder the naming of computer viruses takes the term biology. The main characteristic of a computer virus is that a virus requires a master file to infect when replicating itself, this is what distinguishes computer viruses from other destructive computer programs. Several categories of computer virus are boot virus, program virus, multipartite virus, stealth/polymorphic virus, metamorphic virus and macro virus.The infected master file is called the host file. Today, a computer virus refers to a program that is capable of self-replicating and spreading by duplicating virus codes into the infected file or document.

Keywords: Computer virus, Boot Virus, Program Virus, Multipartite , Polymorphic Virus, Metamorphic Virus and Macro Virus.

INTRODUCTION

The term Virus was first published academically by Fred Cohen in 1984 in his writings. But long before the virus had existed as a game program that was run in a closed computer laboratory.

But long before the virus had existed as a game program that was run in a closed computer laboratory, which at that time was created by computer experts to test their skills. Computer viruses that are created must not leave the computer lab because spreading viruses is categorized as a criminal act.

Every virus that is created will compete, multiply and destroy each other. The virus that survives and dominates is the winner. The term computer virus refers to a program that is capable of self-replicating and spreading by copying virus codes into infected files or documents.

The way it works is identical to biological viruses in general, the virus requires a master file to be infected when replicating itself. The infected master file is called the host file.

Computer viruses have the following capabilities:

- Ability to get information
- Ability to check files/documents
- Self-replicating ability
- Ability to hide yourself
- Manipulation ability

Computer viruses are identical to biological viruses, here's a comparison between the two:

Table 1

Comparison Biological Virus vs Computer Virus

Biological Virus	Computer Virus
Damage only certain cells of living things	Corrupt files with certain formats
In the infected cell, new viruses appear (after the cell is destroyed first - undergoes lysis)	Files/documents that are infected with a virus can transmit the virus to other files/documents
Changing the function of infected living cells	Change the work of files/documents, so that they act like a virus
It's enough that the stem cells are infected with the virus once	In general, computer viruses will only infect files/documents once.
Viruses are capable of mutating and producing variants	Computer viruses are able to change themselves so that it is difficult to detect antivirus programs and the like.
Creatures that are infected do not die immediately	Infected computers/files/documents do not directly show infection damage and can be run within a certain period of time
Requires stem cells for living things to reproduce (infect first)	Requires hosts file to multiply (infect files)

METHOD

Computer viruses have methods of replicating themselves. In general, computer viruses have similarities with biological viruses. Comparison between computer viruses and biological viruses

Viruses are classified according to their action and method of transmission into 7 classifications:

- Boot Virus
- Program Viruses
- Multipartite Virus
- Stealth / Polymorphic Virus
- Metamorphic Virus
- Macro Virus

Many different viruses cause many different symptoms depending on the virus. In general, if there's anything odd about what you're doing, it's probably a sign of viral activity.

Here are the symptoms that are often found on computer systems that are infected with viruses:

- Corrupted data, deleted files and drastically reduced computer performance.

- There is a continuous delay when pressing the keyboard button.
- Computer programs that don't load normally - The hard disk drive is gradually running out of free space.
- The LED light looks like the floppy disk drive or hard drive is running, but the user is not using the storage media.
- New files appear as if they are part of the system files, and the user doesn't feel like installing the files.
- There are annoying beeps on the computer or sounds like pressing a keyboard key for a long time.
- Strange graphic display that appears on the monitor screen
- There are stange files with unknown files names
- Unable to access hard drive while booting from floppy drive.
- Folder Options missing in Tools drop down menu.
- Hidden files cannot be displayed
- Regedit cannot be accessed via RUN box
- Task Manager seems to be disabled by the Administrator.
- Constantly changing program file size
- Computer memory looks much smaller than it should be
- Program acting weird
- The 'Open with' option appears when clicking the drive on the computer.
- Unable to access Command prompt, including Task Manager, Regedit, Msconfig, gpedit.msc; if it can be accessed, immediately close again.

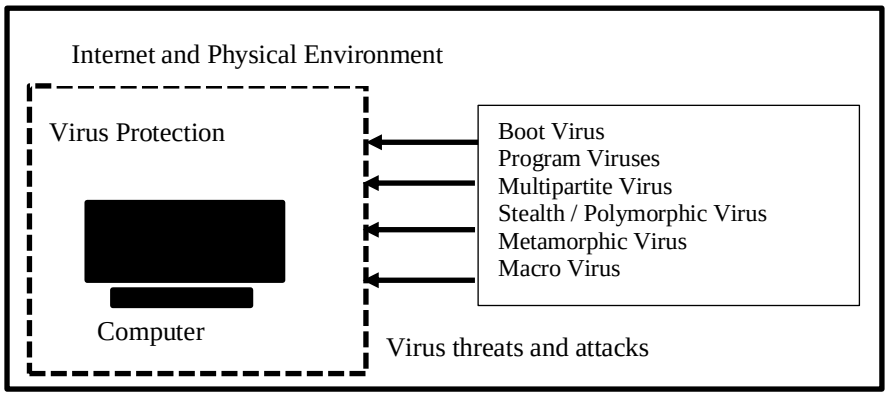

Figure 1. Computer environment and virus threat

Access Penetration of computer viruses through several things, namely:

- Floppy Disks and other storage media
- Internet (files that are downloaded from the internet and then installed so that the virus is not directly activated. Note: browsing the internet will not make the computer infected with a virus)
- E-Mail (Virus wrapped in e-mail attachments. Note: e-mail messages do not contain viruses, only attachment files with the format .exe, .com, bat or other types of executable files that may contain viruses)
- Computer network (for example: when a file affected by a virus is used by many users)

Boot Virus

Boot Sector Virus is able to change the code on the master boot record (MBR) hard disk drive.

The spread is through the boot process, for example booting from a floppy disk infected with a virus, thus the virus will be loaded into memory. This virus will stay in

memory like a device driver. Viruses infect computers by infecting the first hard disk on the computer system.

Maybe you get an error message: "Stop 0x0000007B" error message, as a result of infection with the Secor boot virus on Windows XP. To fix this: do a scan using an antivirus program, but if the antivirus program can't remove the virus and repair the system, repartition and reformat the hard drive, then reinstall the Windows operating system.

Examples of Boot Sector Viruses include: Brian, Stoned, Empire, Form, Azusa, Michelangelo, Polyboot.B, AntiEXE. NYB, and Unashamed.

Virus Program

This type of virus attaches itself to application files, for example files with the format: *.com, *.exe and *.bat.

The virus spreads when the program file is executed, loads the virus coding into memory and copies itself to the program or system. If a file is shared and accessed by many people on a computer network, other computers will automatically be infected. Examples of this type of virus are: The Jerusalem Virus and Cascade Virus

Multipartite virus

Virus Multipartite virus is a combination of boot sector virus and file virus. This type of virus spreads through infected files and storage media and resides in computer memory.

Then the virus will move to the hard drive bootsector, then the virus will infect executable files on the hard drive and spread to other computer systems.

Examples of this type of virus include: the Russian virus, 3APA3A, Ywinz and Tequila

Stealth and Polymorphic Virus

Stealth virus or also known as Polymorphic Virus is generally a boot sector virus, and is able to use certain methods to hide itself from detection by antivirus programs by changing the virus signature. It's also a good idea to install a firewall apart from antivirus software for protection against viruses. Examples of Polymorphic Viruses are: [1], Frodo CivilWar, Silly, Crusher, Ginger, Predator, Satanbug, Tremor, Invisible, Trigger, Uruguay, Basilisk, Scoundrel, and Simulation[2].

Metamorphic viruses

Metamorphic virus, rewrites itself after the transmission process is complete. The method carried out by this virus uses a metamorphic engine, so it is large and complicated, but it is also difficult for antivirus programs to detect. Examples of metamorphic viruses: Win95.Zmist.A[3].

Macro Virus

Macro viruses usually infect document files and spreadsheets, especially in e-mail. Macro viruses are created using macro-based applications. The virus will run the execution automatically when the application where it develops is run and the virus will make many copies of itself[4]

Microsoft provides a version of Visual BASIC in its Microsoft Office products, (eg Word and Excel) so that it allows users to write customized routines. These routines are called macros.

Various macro viruses are written in this language and are included in Word documents, which makes viruses easier to write and execute than other methods.

Examples of macro viruses are:

- The Melissa virus, created in March 1999, spreads to Microsoft Word documents via e-mail. The virus, which was created as a word document, was uploaded to an Internet newsgroup. Anyone who downloads and opens it will trigger a virus. And the virus will send the virus document that is included in the e-mail message to the first 50 people in the address book. Because the action caused large companies to shut down their e-mail systems.

- The ILOVEYOU virus appeared on May 4, 2000. When someone opens the attachment, a virus code will be activated which will send a copy of itself to everyone in the address book and destroy files on the victim's computer.

To avoid the action of macro viruses, use the Macro Virus Protection feature in office applications. With Macro Virus Protection turned on, the auto-execute action will be disabled. Thus, when the document automatically runs the auto-execute regarding the virus code (viral code), the user will be faced with a pops up warning. Don't run macros on documents if you don't know what they do.

IMPLEMENTATION TO PREVENT VIRUS

There are several tips that are quite powerful if applied in preventing the outbreak of computer viruses, including:

- Use Anti-Virus device
- Scan the entire computer on a regular basis
- Update Your Anti-Virus Software regularly, at least once a week.
- Backup files regularly. Always have a copy so that it can be used if the current file is infected with a virus or the computer crashes.
- Turn off E-Mail Preview in mail client settings
- Scan CDs, USB Flash Disks, Floppy Disks obtained from other computers before use. If indeed a virus is found, the anti-virus program will provide options regarding the findings of the virus, such as: remove the virus, do nothing, or delete the file infected with the virus.
- Protect Floppy Disks and USB Flash disks (if there is a protection mode) with Write-protect, this will avoid floppy disks from virus infection, especially boot sector viruses
- Scan files downloaded from the internet before running.
- Scan all E-Mails with Attachments before opening them, generally e-mail viruses reside in attachments.
- Never open an attachment file with a .vbs (Visual Basic Script) or .js (Java Script) file format. Viruses generally hang around with this file
- It's a good idea to subscribe to the virus alert e-mail notification from the antivirus service website.
- To prevent transmission of USB viruses, create an empty file named autorun.inf file, then set the file attribute to read only. This can prevent malicious code from creating autorun.inf.
- Disable Autoplay mode for drive access.
- Antivirus software is a computer program capable of identifying and eliminating computer viruses and other harmful programs such as worms and trojan horses.

Antivirus programs are also able to protect computers from the threat of malicious program attacks. For this reason, antivirus programs must be run regularly so that various computer activities can be monitored (scanned). If a virus is found, the antivirus program can detect it immediately and make further treatment.

The work of Antivirus

Antivirus works by using two methods, namely:

- Dictionary Approach
- Suspicious Behavior Approach

In the Dictionary Approach method, Antivirus Software analyzes every file on the computer and checks its contents using the virus definition reference stored in the virus dictionary.

Virus dictionary is an inbuilt file that is included in antivirus programs, its contents are characteristic information of virus codes that are identified as viruses by antivirus makers.

By using the Suspicious Behavior Approach method, the Antivirus program will constantly monitor the activity of all computer programs. If it is found that a program is trying to write data to the executable file, the antivirus program will flag the program that has suspicious behavior, thus marking the program as a virus.

This method has advantages and disadvantages, the advantage is that computer security can be guaranteed even for all unknown viruses, while the disadvantage is the error in detecting computer programs that are suspected of being viruses, which are actually not viruses. When setting up the Antivirus program with Real-Time Scanning mode, the program will automatically run in the background and scan files and folders as files and programs are opened or executed, this includes downloading e-mail using a mail client program.

Most commercial antivirus software provides real time scanning services. There is no point if the antivirus program is not updated. By auditing the virus dictionary . antivirus programs will be equipped to deal with new malware threats. Commercial antivirus generally provides a daily update mode.

I. CONCLUSION

There are many antivirus programs as well as a variety of business missions, commercial (comercialware) and non-commercial (freeware) and even open source antivirus programs. Antivirus that is classified as open source, for example ClamAV which works very well as an email gateway server, and can also be used on the user's desktop computer. Also moon source antivirus which is opensource. To get an open source antivirus program, freeware or shareware, you can download it on the official website provided or on some mirror downloads.

In addition to downloading the full antivirus program, some antivirus services provide a separate clearner tool that can be downloaded and run specifically to perform cleaning and scans without being applied as a resident antivirus to guard the system 24 hours. Users can try to overcome viruses that attack your operating system using products released by Microsoft, for example the Microsoft Windows Malicious Software Removal Tool which is able to remove specific viruses, such as Blaster, Sasser, and Mydoom, etc.

REFERENCES

1. Subramanya, S.R. and N. Lakshminarasimhan, *Computer viruses.* IEEE potentials, 2001. **20**(4): p. 16-19.DOI: https://doi.org/10.1109/45.969588.
2. Cohen, F., *A cost analysis of typical computer viruses and defenses.* Computers & Security, 1991. **10**(3): p. 239-250.DOI: https://doi.org/10.1016/0167-4048(91)90040-K.
3. Borello, J.-M. and L. Mé, *Code obfuscation techniques for metamorphic viruses.* Journal in Computer Virology, 2008. **4**(3): p. 211-220.DOI: https://doi.org/10.1007/s11416-008-0084-2.
4. Bontchev, V., *Possible macro virus attacks and how to prevent them.* Computers & Security, 1996. **15**(7): p. 595-626.DOI: https://doi.org/10.1016/S0167-4048(97)88131-X.