Awareness about Viruses

Sarika choudhary*, Ritika Saroha, kavita yadav
M.Tech (Network Security)
School of Engg. &Sciences, BPSMV
Khanpur Kalan, sonepat(Haryana)
India

Abstract:

The study of this paper will present perspective view of viruses which can harm our computer system or valuable data. Main focus in this paper on various types of viruses and how they work and what type of methods they use to destroy our data. Aim is to brief discussion about type of viruses so that we can aware about viruses and can protect our system.

Keywords— Virus, worms, OS, Trojan horse, threats.

I. INTRODUCTION

Computer viruses are computer program files or harmless code which enters into the computer without the knowledge of user. They can replicate themselves and spread from one system to another. They affect the program and performance of the system. They can damage data files and another disk by occupying the space on disk and in main memory. Viruses infect another computer by modifying the contents and attaching a copy of itself thus leading to its replication. It is sometime hard to know how a risk must be dealt with before we know its consequences. So viruses should never be leaved on the system. They are very harmful and can destroy many important files. If we copy a virus infected file or damage file so it can harm your other data files, can damage or even delete them. Before studying about the how many type of viruses exist we have to know about the history of viruses.

1.1 History

The first popular computer virus known as "Brain virus" was created in 1986. This was spread via floppy disk. This infects boot records but not hard drives like today's viruses do. This was created by two Pakistani brothers, amjad and basit farooq alvi, so it was also known as the Lahore, Pakistani Brain, Brain-A and it used unused space on the floppy disk for hiding from detection. In 1987, the Lehigh Virus was detected at Lehigh University in US. It was the first memory resident file infector. In 1988, the cascade virus detected at Germany. It was the first encrypted virus. In 2000, the ILOVEYOU virus detected. This was created in the Philippines was sent through e-mail and spread around the world.

II. TYPE OF VIRUSES

There are many types of computer viruses. We can classify these according to their origin, types of operating system attack and their techniques of attack, what type of files they infect, how they damage etc. Here we are describing few of them one by one. These are following:

2.1 Memory Resident Virus

This type of virus is permanent type of virus. It resides in the RAM i.e. volatile memory. When an OS runs they get activated and interrupt all the programs and operations that are opened or executed by the OS. It may take any no. of operations or actions to infect the file and those runs independently on the file. It can corrupt opened, closed or copied or renamed etc. files or programs.

Example: randex, CHJ, meve and marklunky.

2.2 Direct Action virus

As the name suggests this virus take direct action when a specific condition is met. This virus replicates itself and takes action when it is executed. This infects the files and folders in the directory specified in the AUTOEXEC.BAT file path. This file is located into the root directory that is located in the hard disk and this virus will take action at the time of booting. Whenever the code is executed this virus changes their location into new files but in the hard disk's root directory. Basically they corrupt the files so this is file infector virus. This type of virus has done damage in the past.

Example: Vienna virus threatened computer in 1988.

2.3 Overwrite virus

This is the most common virus which operates by infecting the executable files. It copies its code over the computer system's file data, thus deletes the information contained in the file. It can make files partially or totally useless if once they have been infected. This virus replaces the file content so that file cannot be recovered but they do not change the file size. The infected file must be replaced with the clean copy from a backup source. Files that have been corrupted by the overwriting virus cannot be disinfected, we have to delete the complete file and install again.

Example: Way, Trj.Reboot, Trivial.88D, Gorg.202/456, Gorj.377, Loveletter.

2.4 Boot sector virus

This type of virus affects the boot sector of the hand disk. I.e. read by the computer when booting is started. A hard drive has many segments and clusters of segments, which are separated so that portion is called a boot sector. Basically boot sector is a sector in any storage device that contains the booting information. They hide in the memory and when boot data is accessed, they infect it. It came in knowledge when floppy disks were used for booting a system. But now days, this virus is spread by Internet.
Examples: polyboot B, AntiEXE.

2.5 Macro virus

Macro is a series of programming commands i.e. designed by the Microsoft Office. Macro virus is a computer virus i.e. encoded in the Macro and these types of virus attaches itself to a document file such as Microsoft Word and Excel, and has the macro code execute each time the document is opened. This virus can be placed within an ordinary word or excel document and run the macro code when file is opened. Once a Macro virus gets on your computer, it'll infect all the documents you produce. It is created by using the built in Macro Programming language. As soon as document is created or opened, this virus runs and corrupts files and copies itself into other documents. These viruses are also spread through e-mail attachments, modems, internet etc. which we do not expect. It replaces normal macro with Macro-Virus and replace with their same name when we runs that command.
Macro virus executed and file would be infected. This hides in documents that are shared via e-mail or over the internet. 75% of all viruses today are macro virus.
Example: Relax, Melissa.A, Bablas, 097M/Y2K.

2.6 Directory virus

As the name suggest it affects/infects the directories. It changes the directory path that indicates the location of the file. When you try to run a program, you first run the virus program. It infects your file not by changing the file or adding extra file, but by changing the DOS directory information. Once this virus comes in your computer your all directory pointers are changed/infected by it. This virus often uses stealth technology for hiding. This is a type of file viruses but their way of infecting is different. This is also known as cluster virus.
Example: Dir-2 Virus.

2.7 Polymorphic virus

It is very complex virus. After infecting a system it encrypt itself in a different way. It uses different encryption algorithm each time to make copies of itself, which makes it more difficult for a virus detector to detect, or remove. It have hundred and thousand of variants. It basically affects data types and functions. It protects itself with an encryption algorithm which changes itself when specific criteria are met. Example of polymorphism would be if "S" key was switched to "R" or "2" to "3" and so on.
Example: Elkern, Marburg, Satan Bug, Tuarey.

2.8 FAT virus

FAT (File Allocation Table) is the part of hard disk, which is used to store the information about all the file's location, unused space etc. FAT virus make attack on hard disk or specially on FAT(File Allocation Table). It makes files which are stored in hard drive inaccessible. It infects the executable files (.exe) and important files, results in lost information.FAT viruses work in a variety of ways. Some are used to overwrite files and some embedded itself into files so that when FAT file is opened, the virus is triggered. FAT virus is enough powerful to make computer unusable by destroying data and forcing user to reformat.
Example: Link Virus.

2.9 Multipartite virus

It is fast moving and dual personality virus. They spread in multiple ways. It is the combination of two viruses; first one is Boot Sector virus which is used to attack your computer's start-up system and second is file infector which attacks on files. It often infects the hard drive and contains data, which tells machine on how to boot up. It is nasty because of the number of ways they can spread. This virus is also called Hybrid and Multi-part virus. As it has multi-parts so it is difficult to remove.
Example: Invader, Flip, Tequila, Ghostball (was first multipartite virus discovered by Fridrik Skulason in Oct, 1989).

2.10 Web scripting virus

Some websites execute complex code to provide interesting and attractive content. For example: online videos. This needs implementation of a particular code/language to play the video and for helping one who is watching and using video. This code can sometimes be exploited and because of this, it is able to infect a computer system and take actions on a computer system via websites. This particular virus is called Web Scripting Virus. This malicious site is created with the purpose to infect code, and this virus is inserted into the sites with the help of infected code and without the knowledge of webmaster. These sites remains in process without any problem, the fake code takes place under the

webmaster's web control and when any user gives username and password then Hijack/interceptor frame hijack all the information about the user. This type of virus is able to propagate faster than any other viruses.
Example: JS.Fortnight is a virus that spread through malicious e-mail.

2.11 Companion virus

It is an old type of virus that was prominent during the MS-DOS era. This virus stores itself in the file instead of modifying an existing file. It creates a new file similar to original one. This virus infects your file by changing extensions like .EXE to .COM. in command prompt (MS-DOS) when the user executes a program and user types the name of the file without any extension because MS-DOS doesn't need the specification of the file. It automatically runs the first file which matches to the user's given name of the file and you can see companion virus makes sarika.EXE file to sarika.COM so sarika.EXE comes after sarika.COM so MS-DOS executes that sarika.COM file (infected file) first, thus spreading the virus in the computer system.
Example: stator, Asimov.1539 and terrax.1069.

2.12 Parasitic virus

It is a file or programming virus. To propagate, it attaches itself to a file, by splitting in to two parts i.e. pre-pending and appending virus. It keeps most of the file's contents as it is and add pre-pending and appending virus to the start and end of the file respectively. The .COH and .EXE files are simply loaded directly into memory. So they are easy to infect, and execution starts at the first instruction given by the system.
Example: Jerusalam.

2.13 Link virus

It is a file virus. As the name suggests, it doesn't add any code directly into the file in fact it manipulates the way of accessing under the FAT file System. They modify the file pointer so that every program starts from the infected code. When an infected file is run, the virus goes into the memory and writes a code on the disk. Now this file contains a virus code. The virus modifies the pointer to cross-link to the disk that contains the virus code. So whenever, the infected file is run, system jumps first to the virus code and run it.

2.14 Stealth virus

This type of virus is experts in hiding itself. It uses various methods to avoid detection. This is difficult to detect. It hides itself by altering the size of file or concealing itself in memory temporarily. Whenever check is made by any antivirus program for virus then it tells the OS (Operating System) that there is no problem. As a result the anti-virus software can be ignored and this virus continues with their work. This virus is not new in fact; the first computer virus "Dubbed Brain" was a stealth virus.
Example: Dubbed Brain.

2.15 Bounty hunters

This virus can modify antivirus signature so that this'll not able to perform its normal function.

III. WORLD'S WORST VIRUSES

Computer viruses are the nightmares. Some of them can wipe out the information on a hard drive and some can tie up traffic on a computer network for many hours. A fox news report estimated that around $86 billion is lost worldwide annually due to viruses, worms and malwares.
Here we are going to take a look on many worlds' worst viruses in ascending order according to their presence or detection. These ares-

- Malevolent Melissa (March 1999)
- (expletive deleted) Explorer (summers 1999)
- ILOVEYOU and Love Hurts (2000)
- Code red and code red II (2001)
- Tennis anyone? (Feb. 2001)
- The anna kournikova virus (11 Feb. 2001)
- Maniacal Magistr (Mid March 2001)
- Red raider (summer 2001)
- Surreptitious sircam (July 2001)
- Numbing Nimda (Sep. 2001)
- Klz the conquerer (Oct. 2001)
- Bad Benjamin (May 2002)
- Slammer (Jan. 2003)
- SQL spammer/sapphire (Jan. 2003)
- Fizzer (2003)

- MyDoom (1 Feb. 2004)
- Sassor & Netsky
- Poisonlvy (2005)
- Leap –A/ oompa-A (2006)
- Storm worm (late 2006)
- Zeus (2007)
- Agent.btz (2008)
- Conficker virus (2009)
- Stuxnet (2009-2010)
- Autorun

Latest viruses of 2012 are-

- Flame
- Belgian computer crime virus
- Shamon

IV. Other Type Of Malwares And Threats

There are major differences between viruses, worms and Trojans. Worms and Trojans are also a kind of threats. Some are

- Worms
- Trojan horse
- Spywares
- Scarewares
- Logic bombs/Time bombs

V. Conclusion

In this paper we discussed about various types of threats and viruses. If we have the detail knowledge about viruses so we can secure our system very efficiently. This type of deep knowledge about threats or viruses let us move in direction to keep our system very secure. We can provide security to our system to install best updated anti-virus and keep updating it time-to-time.

References

Books:

[1] Security in computing by Charles P. Pfleeger published by Dorling Kindersley(india) Pvt. Ltd.,licensees of pearson education in south asia.

Preferred Sites:

[2] http://www.buzzle.com/
[3] http://www.makeuseof.com/
[4] http://antivirus-software.topchoicereviews.com/
[5] http://www.spamlaws.com/