IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)
An International Open Access, Peer-reviewed, Refereed Journal

COMPUTER VIRUSES: PRINCIPLES OF EXERTION, OCCURRENCE AND AWARENESS

[1]Manishaben Jaiswal

Abstract: computer users including students, home and corporate users, system administrators, corporate managers, and even the anti-virus manufacturers. The viruses are written by people with malefic intentions to bother innocent users. There are many sorts of viruses are boot sector viruses, file viruses, worms, Trojan horses, macro viruses, etc. Each of those has many various variants. Some viruses were transmitting through floppies, boot sector viruses are very rare, but nowadays as nobody boots from floppies. Today, viruses transmit more through networks and emails. Macro viruses are most prevalent within the current days. The viruses generally attempt to exploit the ambiguities of the OS, application programs, windows sockets, and even anti-virus programs. Some viruses are so dangerous that they will make the system completely unusable and irreparable. Nowadays the detection of computer viruses has become common place. In this paper I will like represent principle on which virus is work, how its spread through one machine to another and awareness.

Key words: Virus, computer, e-mail, virus risk, awareness of virus.

INTRODUCTION

Computer Viruses may be a program that copies itself, a bug can infect your computer and slowing down your computer and it also spread computers to computers. The one that sends out the pc (personal computer) virus may use networking of the web. The pc (personal computer) virus can also be spread via disk, CD, that DVD or flash drive or other devices. Computer viruses are usually small, which are designed to spread from one computer to a different computer and to enter and interfere with machine operation. Worm or Trojan is slightly different from another virus it appears harmless, this is often the sort of virus that enters the programs exploits security that may have spread through other networks or Internet users. The virus might corrupt your windows or might delete the important data on your computer, normally virus is often spread through e-mails program to a different computer which may even delete everything on the hard disc. This paper focus on firstly, main principle of the virus and various well-known virus, secondly how the virus spread and finally, the steps which can help to resolve this issue.

1. Principle of computer virus:

Computer viruses spread enormously because they are asymptomatic. In other words, they are difficult to detect. A virus is known as a worm, unwanted computer bug designed to cause damage to computers on a big scale. It widespread like a traditional email attachment, card, or funny image, people are likely to click thereon, and the virus spreads. Additionally, computer viruses also are available in the shape of audio, video, and even anti-virus programs.

Most common virus:

There are various types of the virus, but the most common among them are

Fig 1.0 Virus, Trojan horse, and worm

Viruses: It restricted through small pieces of software that piggybacks on real programs. For instance, it might attach itself to a program like a spreadsheet program. Whenever the spreadsheet program runs the virus runs too, and it is the prospect to breed by attaching to other programs or wreak havoc.

Trojan horses: The program claims to be a game, but instead does damage once you run it, it may erase your hard disk. Trojan horses replicate automatically.

Worms: A worm may be a small piece of software that uses computer networks and security to duplicate itself. A replica of the worm scans the network form an additional machine that features specific security. It copies itself to the new machine using the safety and then starts replicating from there as well.

2. Various types of Virus

File Virus: It infects the system by appending itself to the top of a file. It changes the beginning of a program in order that the control jumps to its code. After the execution of its code, the control returns to most programs. Its execution not even noticed. It also called a parasitic virus because it leaves no file intact but also leaves the host functional.

Boot sector Virus: It infects the boot sector of the system, executing whenever the system is booted and before OS is loaded. It infects other bootable media like floppy disks. These also are referred to as memory virus as they are doing not infect filing system.

Macro Virus: Most viruses written in a low-level language like C or assembly language. This virus was written in an application-oriented language like Visual Basic. These viruses triggered when a program capable of executing a macro run. For instance, the macro virus is often contained in spreadsheet files.

Source code Virus: It is for ASCII (American Standard Code Information Interchange) text file and modifies it to incorporate virus and to assist spread it.

Polymorphic Virus: It is a pattern, which identifies a virus or a series of bytes that structure virus code to avoid detection by antivirus a polymorphic virus changes whenever it installed. The functionality of the virus remains the same, but its signature is modified.

Encrypted Virus: To avoid detection by antivirus, this sort of virus exists in encrypted form. It carries a decryption algorithm alongside it. This virus first decrypts then executes.

Tunnelling Virus: This virus avoids detection by antivirus scanner by installing itself within the interrupt handler chain. Interception programs remain within the background of an OS and catch viruses that become disabled during a tunnelling virus. Similar viruses install themselves in device drivers.

Multipartite Virus: It can infect multiple parts of a system including the boot sector, memory, and files. It is difficult to detect and contain.

3. How does a Virus attack?

Virus attached to a program, file, or document. It will be hidden until circumstances cause the pc or device to execute its code. The virus can remain dormant on your computer, without showing major signs or symptoms. However, once the virus infects your computer, the virus can infect other computers on an equivalent network. Its holdup passwords or data, logging keystrokes, corrupting files, spam your email and contacts. In addition, it takes up on your machine are just a few of the devastating and aggravating things a prevalent can do. Viruses often spread through email and text message attachments, Internet file downloads, and social media fraud links. Mobile devices and smartphones are infected through viruses through app downloads. Viruses can hide disguised as attachments of socially shareable content like funny images, greeting cards, or audio and video files.

While some viruses are often playful in intent and effect, others can have profound and damaging effects. This includes erasing data or causing permanent damage to your hard disc. In worse cases, some viruses designed with financial gains.

3.1 Signs of a computer virus

A virus can spread several symptoms. Some of them are as follows.

3.1.0 Signs of computer virus

- ✓ Frequent pop-up windows, some pop-ups message encourage to you go to unusual sites. Alternatively, they could poke you to download antivirus or other software programs.
- ✓ Changes to your homepage like your usual homepage may change to a different website, as an example. You will be unable to reset it.
- ✓ Mass emails sent from your email account. A criminal may take hold of your account or send emails in your name from another infected computer.
- ✓ Frequent crashes are a virus can impose major damage on your disk drive. This might cause your device to freeze or crash. It is going to prevent your device from returning on.
- ✓ Unusually slow computer performance. A sudden change of processing speed could signal that your computer erections via virus.
- ✓ Unknown programs that begin once you activate your computer. You will become aware of the unfamiliar program once you start your computer. Otherwise, you might notice it by checking your computer’s list of active applications.
- ✓ Unusual activities like password changes. This might prevent you from logging into your computer.

4. Virus risks

Virus attacks more frequently around the world. We should take care of every possible way to remain safe from malicious attacks. Take a glance at a few the highest sources of virus attacks.

Fig 4.0 Virus risks

4.1 Downloading Programs

Programs that contains the downloadable files are the most typical source of malware like freeware, worms, and other executable files. Whether you download a picture editing software, a music file or an e-book. Whenever you notify some unknown, original or smaller amount popular sources then try to avoid it.

4.2 Cracked Software

Whenever you open a cracked software, your antivirus software might flag it as a malware because the cracks contain malicious scripts. Always say "No" to cracks, as they will inject malicious script into your PC.

4.3 Email Attachments

Anyone can send you an email attachment whether you recognize him or her or not. Clicking on unknown links or attachments can damage your system. Consider before clicking anything and confirm that file type is not '.exe'.

4.4 Internet

One of the simplest ways to interact with your device is thru the web. Confirm the URL (Unified resource locator) before accessing any website. For a secured URL always search for 'https' in it. Once you click videos published on social media websites, they'll require you to put in a specific sort of plug-in to observe that video. This plug-in could be malicious software, which will steal your sensitive information.

4.5 Booting Data from unknown CDs

A malicious software can get into your device through an unfamiliar CD. The best practice to be safe from malicious infection is to get rid of CD when your device is not performing at all. Your system could reboot the CD if it is not allow removing before switching off the pc.

4.6 Bluetooth

Bluetooth transfers can infect your system, so it is crucial to understand what sort of media file sent to your computer whenever a transfer takes place. An efficient bulletproof devolve would be to permit Bluetooth connectivity with only known devices and activate it only required.

Apart from above-mention sources, file-sharing networks is a source of bug attacks too.

5 Awareness of the virus issue

There are several ways through which we can save our system and data from the virus interaction.

5.1 Keep your software up so far

Software Company as Microsoft and Oracle update their software on the routine base to repair bugs. That can potential to exploit by hackers. Oracle just released an update to its Java software to repair a security hacker who can want to infect computers with malware.

5.2 Don't click on links within emails

A good rule of thumb is that if you do not recognize a sender of an email then do not click on any links within it. Software company research that 44.8 % of Windows virus infections happen because the pc user clicked on something.

5.3 Use free antivirus software

You do not need to buy software to guard your computer or for an annual subscription to take care of the newest virus protection. For windows users, Microsoft security essentials are free. Avast is another free program.

5.4 Copy your computer

If you have no protection in your system starting from a disk drive, then you must take a backup of your data periodically. Three basic backup options: (1) An external disk drive (2) Online backup service (3) Cloud storage. Use a service like a google drive, google docs, and amazon web services for files open and share. Some cloud storage is free for up to five GB. Some of them are online. Virtual memory is another resource to save your data

5.5 Strong password

While some people use an equivalent password for everything then avoid this practice. Keep the length of the password for is a minimum of eight characters. A strong password including one complex, with a mixture of letters, numbers, and symbols. Switch your password periodically without any reason and safety.

5. 6 Use a firewall

If antivirus software running in your system, then it does not mean you have a firewall. Both PCs and Macs accompany built-in firewall software. Make certain to see that it is enabled.

5.7 Minimize downloads

Your Web browser's security settings are enough strong to detect unauthorized downloads. Keep this setting strong.

5.8 Use a pop-up blocker

Web browsers have the power to prevent pop-up windows and permit you to line the safety for accepting pop-ups, never click on this link. You can use add blocker to block this link which automatically not allow this link to enter into the system.

Conclusion

The computer virus is malicious software programs affecting the web and our computers nowadays. It's become common to possess for a bug found through an email or any sites. People accessing different sites a day should take care of the contents of the page is open. Viruses can damage to your computer or to yourself. Now it should be clear how important to use a computer and keep it safe from viruses. Whenever we use a pen drive or external hard disc you want to scan for viruses to stay your computer safe. Viruses are very destructive programs which will be devastating to companies and individuals. What viruses are, how they get into a computer, how viruses are often avoided, how you get preclude viruses, and therefore the best sort of software want to prevent viruses. We must take care of accessing on-line information, writing a report, and creating a power point presentation.

References:

[1] http://www.mssl.ucl.ac.uk/www_computing/buns/Viruses_demystified.pdf

[2] https://www.reveantivirus.com/blog/en/computer-virus-sources

[3] http://www.mymagicfundas.com/types-of-computer-viruses/

[4] Basu, S. 1997. The Investment Performance of Common Stocks in Relation to their Price to Earnings Ratio: A Test of the Efficient Markets Hypothesis. Journal of Finance, 33(3): 663-682.

[5] Bhatti, U. and Hanif. M. 2010. Validity of Capital Assets Pricing Model. Evidence from KSE-Pakistan. European Journal of Economics, Finance and Administrative Science, 3 (20).

[6] https://www.sophos.com/en-us/press-office/press-releases/1998/08/va_virusesinternet.aspx

[7] https://www.webroot.com/us/en/home/resources/articles/pc-security/computer-security-threats-computer-viruses