DECODING THE WORLD OF COMPUTER VIRUSES: TYPES AND PROACTIVE DEFENSE STRATEGIES

BY *NAVANEETHAKRISHNAN. T*,[1] *MANOHARAN.C*[2] and *VISWAJIT SRINIVASAN*[3]

ABSTRACT

The study aims to investigate the effects of computer virus infections and offer recommendations for safeguarding home computers against such intrusions. In this electronic global community, it is critical to address viral threats and the preventive measures that computer users may take. This technological advancement presents new and adaptable opportunities for measuring security threats to networks. These threats can be either internal or external, with external threats being classified as Trojan horses, worms, hacking, viruses, and so on. Each day, thousands of new and stronger viruses are discovered and released into the wild, but even with this protection, viruses still infect and spread only with the consent of their victims. Following the identification of common causes of computer virus assaults, potential remedies are sent to home computer users in an effort to help them combat these attacks and enhance their computer usage going ahead. This research focuses on the stages of computer viruses, their history, working principles and how to prevent them.

Keywords:

Virus, Antivirus, Threat, Network

I. INTRODUCTION

The purpose of this study is to identify the risk variables for viral assaults among users of personal computers. The usage of computers has dramatically increased in today's culture.

[1] Advocate, Madras High Court Madurai Bench, Madurai
[2] Advocate, Madras High Court Madurai Bench, Madurai
[3] *Student, NALSAR University, Hyderabad.*

Computer virus attacks are more dangerous and cause more visible damage to the system. Analyzing both the actions a virus takes while in a person's system and the potential outcomes over time is crucial. This aids in providing our PC with the necessary security features to protect the confidential data. This study paper's goal is to inform readers on the dangers that computer viruses might pose and offer suggestions for how people can defend themselves against them. These days, a lot of computer viruses are made to quickly multiply and install themselves.[4] It is simpler to restore any documents or programmes that may have been corrupted and stop the virus from spreading if you are aware of the signs of a computer virus and take prompt action to eradicate it from the affected machine.

II. HISTORY OF COMPUTER VIRUS

Viruses have long been spreading over a variety of gadgets through the Internet or other channels. The purpose of the viruses' creation is to steal data, wipe off the device, etc. Launched in 1971 as an experimental self-multiplying virus, the "Creeper system" was the first computer virus ever. Subsequently, the very active Rabbit virus emerged in the middle of the 1970s, rapidly replicating itself and destroying functionality in the process. "Elk Cloner," the original computer virus, was created in 1982 by Rich Skrenta. The device propagated via a floppy disc containing an application and connected to the Apple II operating system. [5]

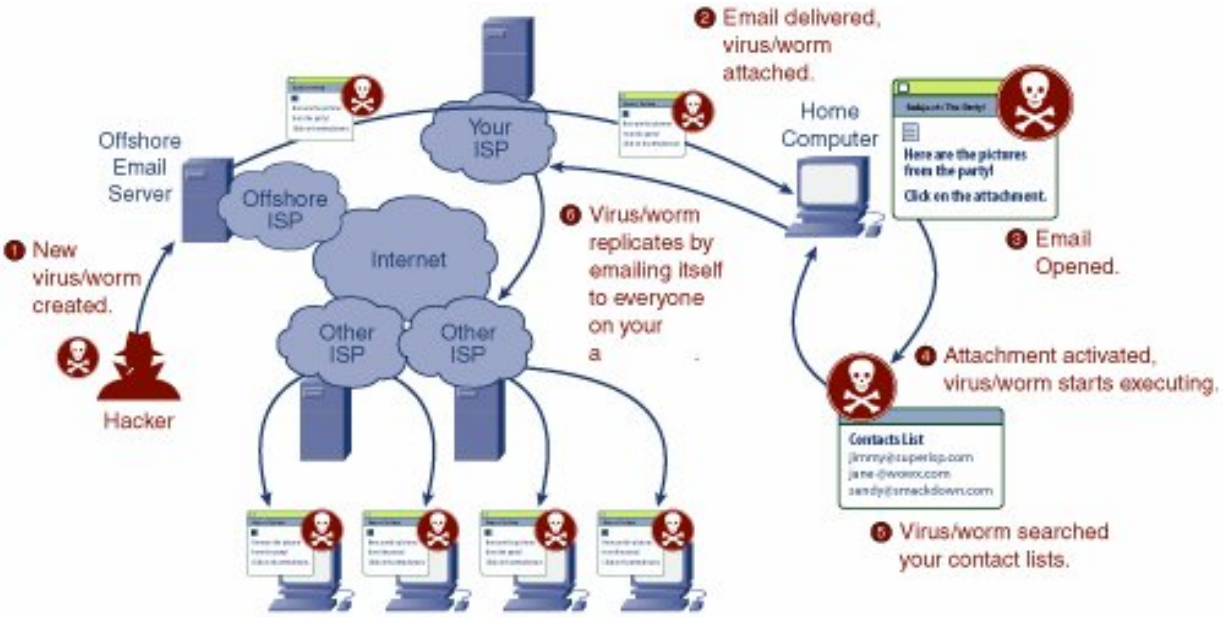
In 1986, "Brain," the first MS-DOS computer virus, was released. The floppy disc's boot sector would be rewritten, making it impossible for the machine to boot up. Two brothers from Pakistan created it with the intention of using it as a copy protection mechanism. The era of devastating viruses started in 1988. Up until then, the majority of infections were essentially jokes with amusing names and messages. "The Morris" was the first virus to spread widely, back in 1988.

III. HOW VIRUSES ATKIN AND SPREAD ON COMPUTERS

[4] Ilmudeen, Aboobucker, The Impact of Computer Virus Attacks and its Preventive Mechanisms among personal computer, (Oct 25, 2023, 2:45 PM), https://www.researchgate.net/publication/326804055_The_Impact_of_Computer_Virus

[5] Sameeksha Khandalwal, what is a computer Virus, (Oct 25, 2023, 3:00 PM), https://www.geeksforgeeks.org/what-is-a-computer-virus/

Floppy discs were used in the early days of computers to transfer viruses from one device to another. While USB devices and hard drives are still common ways for viruses to propagate these days, internet-based device-to-device transmission is more common.



Source: How viruses spread, (Oct 25, 2023), **https:// flylib.com/books/en/2.282. 1.25/1/**

Email is a common way for computer viruses to spread; some of them may even take over email programmes to propagate. Other viruses can be obtained from hacked application shops and infiltrated code repositories, and they can connect to or infect genuine applications, software packs, or code. Any computer virus must have the host programme active in order for the victim to execute its code, or payload.

IV. TYPES OF COMPUTER VIRUS

They are millions of different kinds of viruses in the globe, here are some common ones you should know about. [6]

- **File-Infecting Virus**

[6] What are the different types of Computer viruses, Uniserve, (Oct 25, 2023, 4:00 PM) https://uniserveit.com/blog/what-are-the-different-types-of-computer-viruses

An executable programme attachment virus, also known as a parasitic virus, usually infects files with the.exe or.com extension. Some file infectors have the ability to replace host files, while others can corrupt the formatting of your hard drive.

- **Macro Virus**

  Programmes like Microsoft Word and Excel are frequently infected with this kind of malware. These viruses are typically kept as a component of a document and can proliferate when files are sent to different computers, frequently via email attachments.

- **Browser Hijacker**

  This malware targets and modifies the settings of your browser. Because it reroutes your browser to other harmful websites that you don't intend to visit, it is sometimes referred to as a browser redirect virus. Other dangers this malware may provide include altering your browser's default home page.

- **Web Scripting Virus**

  An exceptionally cunning malware that targets well-known websites. By inserting links that might install malicious software on your device, this virus replaces code on websites. Cookies can be stolen by web scripting viruses, which then utilize the data to post content on the compromised website on your behalf.

- **Boot Sector Virus**

  When computers were booted from discs, these viruses were formerly rather widespread. These days, tangible devices like USBs and external hard drives are used to spread these diseases. In the event that your computer has a boot sector virus, it loads into memory automatically and gives you control.

- **Polymorphic Virus**

  As it may alter codes each time an infected file is executed, this virus can elude detection by anti-virus software.

- **Resident Virus**

  A resident virus can infect files on your computer by storing itself in the memory of your machine. This virus has the ability to damage files and programmes by interfering with your operating system.

- **Multipartite Virus**

  A particular kind of virus that spreads quickly across your computer system and is very contagious. It is challenging to contain as it may infect memory, files, and the boot area of a machine.

V. SYMPTOMS OF COMPUTER VIRUS INFECTED IN SYSTEM

It is advisable that you take action if you observe any or all of these symptoms, since your computer may be infected.

- Unexpectedly sluggish computer performance, with programmes taking substantially longer to launch or start up.
- Issues with unexpectedly shutdown the system or restart the system.
- Files Missing.
- Recurring system failures.
- Recurring notifications for errors.
- Unexpected pop-up windows.
- Emerging programmes (such as toolbars for web browsers) that show up without needing to be downloaded.
- An overworked hard drive might be identified if the internal fan on your device seems to be humming and straining excessively while you're not using it.
- Emails that are sent from your accounts automatically and without your intervention.
- slow-loading browser or one that keeps rerouting you.

- firewalls or antivirus software not working properly[7]

VI. METHODS TO PREVENT COMPUTER VIRUS[8]

- **Set up an antivirus software**.

  It is important to have dependable security whether or not you are linked to the internet. Make sure you are secured as soon as you turn on your computer by investing in antivirus software, which only costs a few dollars.

- **Set up anti-malware and anti-spyware software**

  Numerous of these programmes are free and guard your PC against viruses. When utilized properly, they fulfil their intended purpose, however they do require constant operating and update.

- **Stay away from suspicious websites**

  Websites usually alert you when they try to install or execute a programme on your computer, but this isn't always the case. Stay away from those kinds of websites.

- **Email attachments should always be screened before opening**

  Email is still the most prevalent method used to distribute viruses. Use an email service that mandates that all attachments be checked before opening in order to protect your machine from viruses. Too many individuals will open an attachment without second thought because they immediately believe that it is secure if it shows up in their work email inbox.

- **Configure automated scanning**

  It's a good idea to schedule regular or weekly computer scans to remove any infections. This maintains your computer up to date and error-free.

[7] How to tell if your computer has a virus and what to do about it, NCA, https://staysafeonline.org/online-safety-privacy-basics/how-to-tell-if-your-computer-has-a-virus-what-to-do-about-it/

[8] Ways to protect your computer from virus, https://www.chicagoitsolutions.com/2022/07/22/11-ways-to-protect-your-computer-from-viruses/

- **Observe the downloads**

  We know that a lot of us download items from the internet, including movies and music, but a lot of us also end ourselves in problems for doing so. Such large files can easily include malicious content, so be cautious about what you download.

- **Update**

  "Critical Update" for Microsoft Windows is one example of being one step ahead of cybercriminals. Microsoft has a whole division called Critical Update that is devoted to preventing viruses from infecting PCs. Keep your system updated at all times.

- **Always be aware**

  Regardless of your level of computer usage—casual or enthusiast—you should constantly be aware of the most recent viruses and how they might impact your system. This will help you be ready for any eventuality so that you can address the issue more quickly. Be careful to be vigilant if you learn of a virus that is spreading like wildfire. Avoid downloading anything, and use additional caution while opening files and emails.

- **Multi Factor Authentication**

  When you connect into your email account (or other services like remote access to a network), multi-factor authentication adds an extra degree of security. After entering your login credentials and receiving a code by text message or an app on your phone, you are required to input another code. In this manner, even if the bad guys manage to get their hands on your password, they won't be able to access your phone and therefore, log in. Everyone is aware that downloading software that is unauthorized or "cracked" from the internet may appear to be more cost-effective, but in actuality, it can be harmful. They push your computer through difficult-to-find faults and will ultimately lead to further issues for you.

- **Setup firewall**

  An application that filters incoming network and internet traffic is called a firewall. It can assist in preventing unwanted access to your computer in addition to your antiviral programme.

- **Educate Your Employees**

  The best thing you can do to maximize the return on your investment in IT security is to educate your staff about the threats that exist on the internet. Instruct them on security best practices so that they don't become additional risks to be aware of, but rather become a part of your network security solution.

VII. CONCLUSION

In conclusion, the proliferation of personal computers in today's society has brought with it a host of security challenges, with computer viruses posing a significant risk to users and their valuable data. The history of computer viruses underscores the evolution of these threats from experimental self-multiplying programs to more sophisticated and potentially devastating malicious software. Ultimately, computer security is a shared responsibility that extends to both individual users and organizations. By implementing these preventative measures and staying vigilant, we can collectively reduce the risk of falling victim to computer viruses and ensure the safety of our digital lives in an increasingly interconnected world.