International Journal of Scientific Research and Engineering Development-– Volume 6 Issue 2,Mar-Apr 2023

Available at www.ijsred.com

RESEARCH ARTICLE OPEN ACCESS

Hazard of Computer Viruses

Samruddh Uchil

*(Department of Information Technology, KSD's Model College, Dombivli

Email: samruddhuchil.model@gmail.com)

----------**********----------

Abstract:

Computer viruses are nefarious software applications that have the potential to seriously harm computer networks, systems, and data. The objective of this paper is to offer a thorough analysis of the literature on the dangers of computer viruses. The paper examines the development of computer viruses, how they spread, and how they affect computer systems. The many sorts of viruses, including Trojan horses, file infectors, macro viruses, and boot sector viruses, are also covered in the article along with their possible risks. The report also describes the precautions that can be taken to avoid contracting viruses, including the use of firewalls, antivirus software, and safe passwords.

Keywords **—Computer viruses, networks, data.**

----------**********----------

I. INTRODUCTION

Computer virus spread has grown to be a major issue for people, companies, and governments all around the world. Computer viruses are harmful software applications created with the intention of contaminating computer systems, networks, and data. They may result in a variety of issues, such as data loss, system breakdowns, and identity theft. The purpose of this paper is to present a thorough analysis of the risks posed by computer viruses, their methods of propagation, and their possible hazards.

II. HISTORY OF COMPUTER VIRUSES

A programmer named Bob Thomas invented the first computer virus in 1971. Its goal was to infect mainframe machines running the TENEX operating system. The virus's name was Creeper. Viruses evolved and spread more widely in the years that followed. The propagation of viruses via floppy discs and email attachments started in the 1980s. The Internet had developed into a significant channel for virus propagation by the 1990s.

III. MODES OF TRANSMISSION

Email attachments, infected websites, infected software, and infected USB devices are just a few of the ways that computer viruses can spread. Peer-to-peer networks, instant messaging, and social media are additional channels through which they can spread. Once a computer has been infected, the virus can spread to further computers connected to the same network and, in certain situations, to machines connected to different networks.

IV. TYPES OF VIRUSES

Computer viruses come in a variety of forms, each with specific traits and dangers. The most prevalent kinds include Trojan horses, file infectors, macro viruses, and boot sector viruses. A hard drive's boot sector can become infected by boot sector viruses, which makes it challenging to start the machine. Executable file infectors affix themselves to them and can seriously harm the system. Spreadsheets and documents can include macro viruses that can corrupt data. Trojan horses are malicious programmes that are concealed within normal software and can damage the system.

V. POTENTIAL DANGERS

Computer viruses have the potential to seriously harm networks, data, and computer systems. Data loss, system malfunction and identity theft may result from them. Additionally, they have the potential to undermine network security and give hackers access to private data. In addition, viruses have a high rate of dissemination, which can result in extensive illnesses that take days or even weeks to resolve.

VI. PREVENTION

The usage of firewalls, antivirus software, and strong passwords is the most efficient strategy to stop infection by viruses. Before viruses seriously harm the system, antivirus software can find and get rid of them. Secure passwords can shield critical information from hackers, and firewalls can stop unauthorised users from accessing the network. Additionally, it is crucial to keep software updated because security patches that fix known vulnerabilities are frequently included in software updates.

VII. EFFECTS OF COMPUTER VIRUSES

Computer viruses are a sort of malware that can affect networks and computer systems in a variety of ways, notably by stealing data, crashing systems, and allowing unauthorised access. The following figures highlight some of the serious concerns associated with computer viruses:

1. The FBI stated in 2020 that it received more than 2,000 reports per day about cybercrime, including malware, which caused more than $4.2 billion in losses.
2. The average cost of a data breach brought on by a virus or another form of malware was $4.24 million, according to an IBM analysis from 2021.
3. Sixty-six percent of IT professionals surveyed by the Ponemon Institute in 2021 said their companies had experienced a data breach brought on by a virus or other malware in the previous 12 months.
4. A study by AV-TEST, a reputable IT security organization, found that just in 2020, there were more than 1 billion new malware threats.
5. Cybersecurity Ventures predicted in 2020 that by 2023 the cost of cybercrime, including viruses and other forms of malware, would exceed $6 trillion globally.
6. These statistics highlight the significant hazards associated with computer viruses and the importance of taking measures to protect computer systems and networks from these threats.

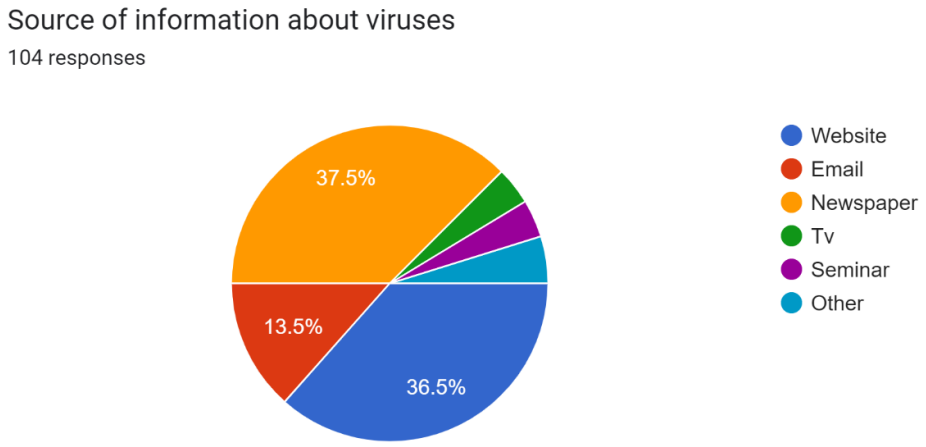
VIII. HOW TO PREVENT AN ATTACK

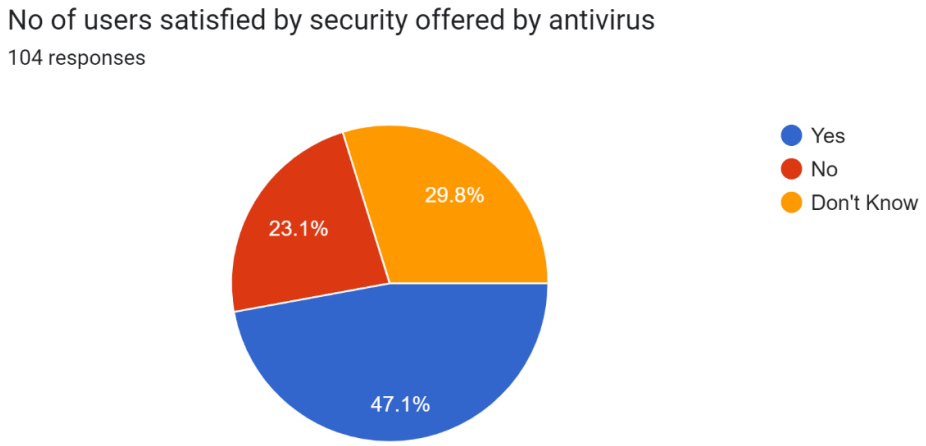
- Update your operating system regularly. It blocks security holes that can be exploited by viruses or hackers.
- Update your Anti-Virus. Don't rely on the automatic updates. Open the Anti-Virus program, check when the last update was performed and if necessary check for updates manually. Make sure the program and the virus definitions are both constantly updated.
- Update all Software. Try to keep all your software updated. Every program nowadays has an online connection, which can mean a gateway for spyware adware etc to get in. This is mostly true for browsers. So, make sure you have the latest version.
- Don't click on links sent to you by e-mail by an unfamiliar sender as this is a common way for malicious website to hook you in. Instead go to the browser and type in the websites name in directly.
- Avoid Bad websites like adult sites, piracy sites and file sharing sites. Any website where you get a continuous number of pop up pages on any link you press is generally bad and should be avoided.
- Be careful when installing Programs. Always research any programs you wish to install. Do not install a program just because it appears to suit your

needs. If it is a good program there will be many reviews and recommendations.

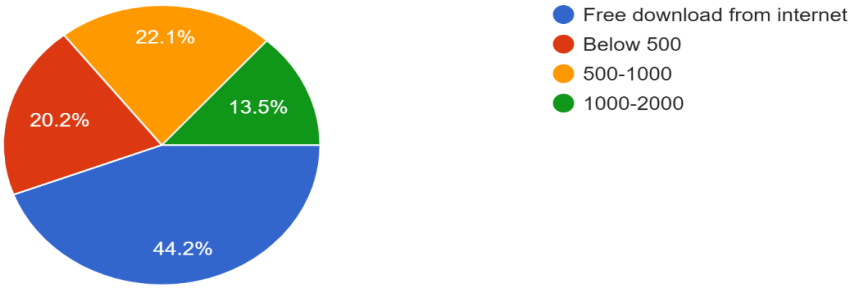
- Avoid Clicking Popup adverts. If you're careful and you know the website is legitimate then it can be okay, but a lot of the time they're not and are to be avoided. Specifically, ones that say they will improve your computer.
- Be Vigilant. If you get a window pop up that looks like it's scanning your hard drive for viruses or errors, yet you have never seen this program before close it instantly.
- Run Virus clean up regularly. Most antivirus programs have a scheduler that will schedule a regular scan of your computer. Make sure this is enabled, and check regularly to see if it has been run.

Survey Results:

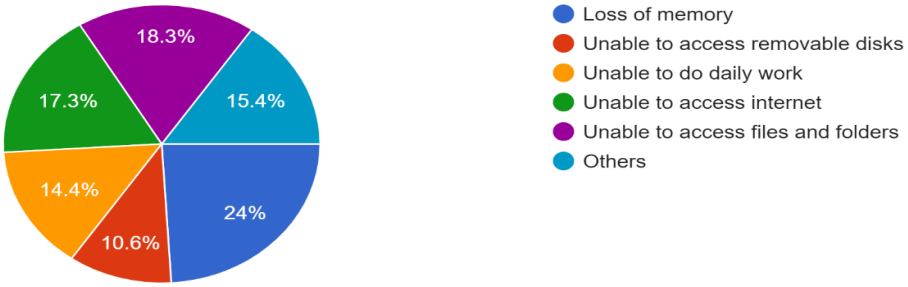




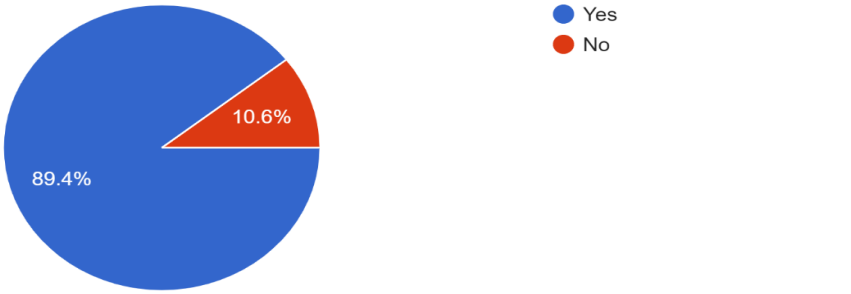
Amount users are willing to spend on antivirus software
104 responses



Effects of virus activities
104 responses



People willing to know about viruses
104 responses



IX. CONCLUSIONS

A major threat that can seriously harm computer systems, networks, and data are computer viruses. It is crucial to take precautions against virus infestations, such as by utilising firewalls, antivirus software, and secure passwords. Individuals, corporations, and governments can safeguard themselves from the perils of this quickly growing menace by being aware of the risks posed by computer viruses and taking proactive actions to prevent infestations.

REFERENCES

[1] Computer Virus Strategies and Detection Methods Essam Al Daoud,, Iqbal H. Jebril2 and BelalZaqaibeh Int. JOpen Problems Compt. Math., Vol. 1, No. 2, September2008 pg 122- 9)
[2] User Knowledge and Attitude of Computer Viruses inMalaysiaMadihah Saudi , Shaharudin Ismail, Muhammad NajibMasdan International Journal Of Learning, Volume 13, Number 8, 2006 Pg 111-122)
[3] Computer Viruses and Challenges for Anti-virus Industry Deepak Kumar ,Narender Kumar , Aditya Kumar International Journal Of Engineering And Computer Science ISSN:2319-7242 Volume 3 Issue 2 February , 2014 Page No. 3869-3872.
[4] Computer Viruses: How to Avoid Infection http://www.msubillings.edu/cotfaculty/security/alviruses.pdf pg 1-6)
[5] Bits & PC‟s 10 Step Guide to Protect Against Viruses (2012,march 4) http://www.bapcs.co.uk/10-stepguide-to-protect-against- viruses [7] DanchoDanchov. 20 Jul 2004. Reducing “Human Factor” Mistakes. Article in MISC Network Security.(2003,July23)(online)http://www.windowsecurity.com/articles/Reducing_Human_Factor_Mistakes.html

