Journal of Progress in Engineering and Physical Science
ISSN 2709-4006
www.paradigmpress.org/jpeps
Volume 5 Number 2 June 2026

Computer Virus: An Analysis on Detection and Prevention Technology

Haradhan Kumar Mohajan[1]

[1] Chairman and Associate Professor, Department of Mathematics, Premier University, Chittagong, Bangladesh
Correspondence: Haradhan Kumar Mohajan, Chairman and Associate Professor, Department of Mathematics, Premier University, Chittagong, Bangladesh.

doi:10.63593/JPEPS.2026.06.06

Abstract

A computer virus is a destructive computer program that can spread across computers and networks by making copies of itself to a host file or system area commonly through the email attachments, usually without the users' knowledge and runs against wishes of users. It attaches itself to files, programs or parts of the operating system and performs harmful actions, such as delete of files, slowdown of the computer, corruption of data, steal of sensitive information, damaging computers and computer systems, etc., of individuals and organizations. It is the most potent and vulnerable threat for computer users that hampers important work involved with data and documents. It has replication, protection, and payload mechanism. It is potentially dangerous that can threaten the proper functioning of the computer system. Once it gets control, it multiplies itself to form newer generations. An attempt has been taken here to discuss the detection and prevention strategies of computer viruses.

Keywords: computer virus, anti-virus, cyber security, cyber threat

1. Introduction

Malware is malicious software that is designed to harm or exploit devices. In general, malwares include worm, botnet, virus, Trojan horse, backdoor, rootkit, logic bomb, rabbit, spyware, etc. (Zeidanloo et al., 2010). It is wide-ranging and its capabilities are quite extensive that can crack weak passwords, lock up files, spam, and can spread through networks. Its attacks can lead to data theft and the destruction of entire computer system (Wang et al., 2018). A computer virus is a type of malware that replicates itself by modifying other computer programs, inserting its own code into host program. It spreads from device to device when infected files are shared through the pen drives and emails (Gole, 2024). It is designed to cause harm for corrupting data, slowing down systems, stealing personal information, destroying data, smash up hard disk space, etc. (Burger, 1991). To escape generic scanning, a virus can modify its code and alters its appearance on each infection. Like biological virus, computer virus is contagious, stealthy, infectious, latent, excitable, expressive, and destructive (Zhang, 2022).

The term "computer virus" was coined by American computer scientist Fred Cohen in 1985 and has been borrowed from biological science

with almost similar meaning and behavior. The only difference is that the victim is a computer system and the virus is malicious software (Cohen, 1984). Viruses can increase their chances of spreading to other computers by infecting files on a network file system or a file system that is accessed by another computer (Zeidanloo et al., 2010). Virus writers use social engineering deceptions and exploit detailed knowledge of security vulnerabilities to initially infect systems and to spread the virus (Stallings, 2012). Although all of them are malware, their behaviors are different and their patterns of infection and transmission are also different (Mishra, 2012b).

There are two types of computer viruses: simple viruses and encrypted viruses. A simple virus that merely replicates itself is the easiest to detect. When a user launches an infected program, the virus controls the computer and attaches a copy of itself to another program file. After it spreads, the virus transfers control back to the host programs and functions normally (Dixit et al., 2012). On the other hand, an encrypted virus consists of a virus decryption routine and an encrypted virus body. If a user launches an infected program, the virus decryption routine first gains control of the computer, then decrypts the virus body, and then decryption routine transfers control of the computer to the decrypted virus (Wang et al., 2018).

Most email viruses are disguised in a very attractive manner, such as photos, audio and video files, e-greetings cards, etc. (Mohajan, 2025a). About 50,000 computer viruses provide a variety of effects ranging from the merely unpleasant to the catastrophic situation, and some of them are boot sector virus, file virus, resident virus, non-resident virus, macro virus, polymorphic virus, hoax virus, Trojan horse, spyware, backdoor, worm, hoax, key logger, adware, jokers, partition sector virus, test virus, logic/time bomb, multipartite virus, etc. (Ludwig, 1996). Some well-known viruses in attractive names are CryptoLocker, amoeba, ILOVEYOU, KISS ME, MyDoom, Sasser and Netsky, Slammer, Stuxnet, etc. (Polk et al., 1995).

2. Literature Review

A literature review is a comprehensive survey of academic sources, such as books, journal articles, theses, etc. On a specific topic that offers a critical analysis, synthesis, and overview of previously published works (Creswell, 2013). It provides the researchers and the audiences with general information of an existing knowledge on a particular topic (Galvan, 2015). It is a more or less systematic way of collecting and synthesizing previous research (Torraco, 2016). It is an excellent way of synthesizing research findings to show evidence on a meta-level and to uncover areas in which more research is needed that is a critical component of creating theoretical frameworks and building conceptual models (Hannah, 2019).

Harold Joseph Highland has discussed on the three computer viruses: Brain or Pakistani virus, Lehigh or COMMAND.COM virus, and Israeli virus. The Brain virus was a boot sector infector. The Lehigh virus and the Israeli virus infected executable code; the former attached itself only to COMMAND.COM, and the latter infected .EXE and/or .COM programs (Highland, 1997). Devkumar Gole has presented what is a virus, history of virus, how does a virus infected computer, how can we detect a virus infected computer, how do we protect our computer against viruses, specific types of viruses, and what is an anti-virus (Gole, 2024). Nitesh Kumar Dixit and his coworkers have presented a general overview on computer viruses and defensive techniques. They have observed that computer virus writers commonly use metamorphic techniques to produce viruses that change their internal structure on each infection. On the other hand, anti-virus technologies continually follow the virus tricks and methodologies to overcome their threats (Dixit et al., 2012).

Vivek Kumar has shown that a computer virus is a type of malicious software that spreads between computers and causes damage to data and software. The virus is attached to an executable host file that results in their viral codes executing when a file is opened. The code then spreads from the document or software it is attached to via networks, drives, file sharing programs, or infected email attachment, and can reproduce itself in the same or other form (Kumar, 2024). Hossein Rouhani Zeidanloo and his coauthors have observed that among the diverse forms of malware, botnet and worm are the most widespread and serious threats that occur commonly in most of the cyber-attacks (Zeidanloo et al., 2010).

Milind. J. Joshi and Bhaskar V. Patil have highlighted on the computer virus, history of worst computer attack, and type of computer virus with effect on computer and few examples

of virus on their types, working of computer virus, and problem occur due to virus in computers (Joshi & Patil, 2013). Babak Bashari Rad and his coworkers have reviewed new methodologies and have outlined their strengths and weaknesses to encourage those who are interested in more investigation on these areas to make them stronger, more and more, every day (Rad et al., 2011).

3. Research Methodology

Research is the systematic and diligent investigation into a subject to discover, revise, or interpret facts, theories, and applications (Kara, 2012; Mohajan, 2018a). It involves the collection, organization, and analysis of evidence to increase understanding of a topic, characterized by a particular attentiveness to control sources of bias and errors (Roffee & Waling, 2016). The primary purposes of research are documentation, discovery, and interpretation of methods and systems for the advancement of human knowledge (Rocco et al., 2011). Methodology is a systematic and theoretical analysis of the methods and principles associated with a branch of knowledge (Franklin, 2012). It indicates various theoretical commitments about the intended outcomes of the investigation (Howell, 2013). Therefore, research methodology is the systematic and theoretical analysis of the methods applied to a field study, outlining the procedures, tools, and techniques for collecting and analyzing data (Bhome et al., 2013).

We have used secondary data to prepare this qualitative research paper. It can identify the domain, selection, designing and inclusion of various measuring variables in any research. For the collection of secondary data, we have used both published and unpublished data sources related to computer virus. We have unsparingly consulted valuable articles and books of famous authors. We have also collected some materials from the internet and websites (Mohajan, 2017, 2018b, 2020). In this study, we have dealt with some computer virus related qualitative research materials, such as historical background and characteristics of computer virus, various types of computer viruses that are harmful for computer, and protection policy of computer from virus attacks.

4. Objective of the Study

Computer viruses are special kinds of computer programs that spread across disks and networks by making copies of them (Mohajan, 2025b). They are malicious programs that either activate immediately or lie dormant until triggered. They can self-replicate, inserting themselves onto other programs or files, infecting them in the process. They have the ability to get information, check files and documents, hide themselves, and manipulate the programs (Wang et al., 2018). Disasters caused by viruses are damaging of programs and software, deleting of files and data on storage devices, corruption of files, slows down of the speed of the computer, formatting of the hard disk, booting failure, taking up of computer memory, and causing of the system crashes (Kephart & White, 1993). They can write their own codes into the host program, and can infect a computer without permission of the user (Kumar, 2024). At present different unauthorized users hacked our important files, folders and emails through the different worms, viruses, and spam mails (Gole, 2024). Main objective of this article is to discuss the aspects of computer viruses in some detail. Some other minor objectives of the study are as follows:

1) to highlight on the historical background of computer virus,
2) to show the characteristics of computer virus,
3) to analyze the various types of computer viruses, and
4) to discuss the protection of the computer system from virus attacks.

5. Historical Background

A computer virus is a malware that replicates itself by modifying other computer programs and inserting its code. It comes in different types, and each type can affect the devices differently. It is the most well-known form of malware that is designed to disrupt a computer system operation (Aycock, 2006). It results in the loss or damage of hardware, software, data, information, or processing capability of a computer or mobile device. For example, in 1999, the infamous Melissa virus infected thousands of computers and caused damage close to $80 million; while the Code Red worm outbreak in 2001 affected systems running Windows NT and Windows 2000 server and caused damage in excess of $2 billion (Markoff, 1999).

In 1949, Hungarian and American mathematician, physicist, computer scientist, and engineer John von Neumann (1903-1957) has designed a self-reproducing computer program

that is considered the first computer virus of the world, and he is considered to be the father of computer virology. His seminal work was published as the "Theory of Self-Reproducing Automata" (von Neumann, 1966). In 1972, Veith Risak has been directly building on von Neumann's work on self-replication published his article "Selbstreproduzierende Automaten mit minimaler Informationsübertragung" (Filiol, 2005). The Creeper virus was first detected on ARPANET, the forerunner of the internet, in the early 1970s that could copy itself. It was an experimental self-replicating program written by Bob Thomas at BBN Technologies in 1971. In the mid-1970s, the "Rabbit" virus emerged that replicated very quickly and caused significant damage at the same pace, but it does not necessarily spread over the network (Parikka, 2007). Rabbit is also called Bacteria, is a malicious code that mainly designed to use up large amounts of system resources, such as message buffers and file space by creating many instances of it or run many times simultaneously (Zeidanloo et al., 2010).

In 1982, Elk Cloner personal computer virus was appeared that was written in 1981 by Richard Skrenta, a ninth grader at Mt. Lebanon High School near Pittsburgh. It spreads through a floppy disk containing a game and attached itself to the Apple II operating system (Jesdanun, 2007). In 1983, the first computer virus was designed and tested by American computer scientist Fred Cohen, and the virus was demonstrated as VAX 11/750 system that crashes the computer within 30 minutes. In 1984, he has written a paper "Computer Viruses: Theory and Experiments" (Cohen, 1984). Two years after the release of Windows 3.0, first virus to specifically targeted Microsoft Windows, WinVir was discovered in April 1992 (Miller, 1996).

The first IBM PC compatible virus in the "wild" was a boot sector virus named Brain or Pakistani virus was created in 1986 and was released in October 1987 by two brothers Amjad Farooq Alvi and Basit Farooq Alvi in Lahore, Pakistan. It struck at the University of Delaware in the USA outside of a test laboratory. It has also struck at many universities of the world and even some businesses, such as the Journal-Bulletin in Rhode Island in the USA (Highland, 1997). One month later, the Lehigh or COMMAND.COM virus was discovered at Lehigh University in Pennsylvania. In December 1987, the Hebrew University at Jerusalem discovered that its microcomputers had been infected by a computer virus in .EXE and/or .COM programs. In 1988, "The Morris" became the first widely spreading virus (Polk et al., 1995).

Upon closer examination the computer specialists under Yisrael Radai of the Computation Center of the University found that every time an .EXE QQAQA executed, and its size increased by 1808 bytes. The .COM programs increased in size as well but there was only a one-time increase. In February 1996, Australian hackers from the virus-writing crew VLAD created the Bizatch virus that was the first known virus to specifically targeted Windows 95 (Yoo, 2004).

6. Characteristics of Computer Virus

A computer virus is a malicious code that replicates and spreads, which is characterized by its ability of attachment to clean files, trigger harmful actions, and hide from antivirus software; and requires user interaction to activate, leading to erratic behavior, crashes, and unauthorized activity (Aycock, 2006). The harmful effects caused by viruses are (Dixit et al., 2012) i) corruption of executable program files, such as word processors, operating system, etc., ii) delete of information from files, iii) increase of the size of files by attaching themselves to those files, iv) monitoring activity and stealing important data, such as credit card information, account number and password, and v) formatting the hard disk for destroying the data (Polk et al., 1995). A computer virus has many characteristics, and some of them are as follows (Mohajan, 2025c):

6.1 Self-Replication Mechanism

The virus has the ability to replicate itself to infect computers, as like its biological counterpart. A self-replicating computer virus is a type of malicious software that upon execution, replicates itself by modifying other computer programs and inserting its own code. It can reproduce and spread automatically (Sayama, 2006). It can copy itself into other executable files, boot sectors, documents with macros, scripts or memory (Kim & Solomon, 2010). The replication may be immediate, delayed, or conditional. By replicating itself it is able to spread across computer systems and networks to infect as much as it possibly can. It requires a host that is executable, document, boot sector, and script to carry and run its code, and some common hosts are .exe/.dll files, Office Macros, PDF/JS, boot

records, interpreted scripts, etc. (Wang et al., 2018).

6.2 Executable Path

An executable virus is a non-resident computer virus that stores itself in an executable file and infects other files each time when the file is run. At the starting, the virus must execute itself with infected host to run a program. Its path is not limited to a single location, as it often disguises itself as legitimate files or hides within system folders to evade detection (Yoo, 2004). The virus typically attaches its code to a host file with .exe, .com or .scr extensions and executes by attaching to or replacing legitimate executable files when that file is opened. It can install auto run entries, modify startup scripts, and infect boot sectors to survive reboots (Khan, 2012). It can install itself into Windows system directories to appear legitimate, such as C:\Windows, C:\Windows\System32, or C:\Program Files. Instead of a traditional file path, it targets the hard drive's Master Boot Record (MBR), placing the code at the very beginning of the drive partition to run before the operating system (OS) loads (Arnold & Tesauro, 2000).

6.3 Malicious Payloads

A malicious payload is a code that is responsible for malicious activities and a virus may perform it. It is the component of malware, such as viruses, worms, or Trojans that executes harmful activities, such as file deletion, disk corruption, data wiping, data theft, file destruction, or encryption (Hasan et al., 2020). It ranges from the virus that overwrites or deleted files on the system, such as overwriting the Flash Bios of system or overwriting special media file types to a new type of virus that is not designing for damaging files on the system, but allowing backdoor access to the system for stealing sensitive information, such as passwords (Zeidanloo et al., 2010). The disruptive features are crashes, system instability, and denial of service. The stealthy ways are backdoors, keyloggers, and data exfiltration. Other informational activities are messages, altered UI, etc. The virus lies dormant until triggered, often delivered via phishing, malicious links, or software vulnerabilities (Rajesh et al., 2019).

6.4 Side-Effects

With the self-replicating code, the virus contains a payload that is similar to a warhead on a missile, which is called the side-effect of the virus. The payload has the potential to be malicious, but it does not have to be (Joshi & Patil, 2013). Main side-effects are performance degradation, hijacked browsers, unexpected pop-ups, high resource usage, corrupted files, unauthorized network traffic, disabled security software, unauthorized emails sent to contacts, and compromised confidentiality (Wang et al., 2018). The key side-effects of a computer virus are system performance degradation that makes the computer becomes very slow, freezes often, or takes a long time to open files or programs (Abdulmalik, 2024); data loss or corruption that the files may disappear, become encrypted, or get corrupted, leading to permanent data loss; system instability that frequent crashes, the "blue screen of death", or unexpected shutdowns/restarts (Oyelere & Oyelere, 2015); malicious activities that the computer may display unwanted ads, send unauthorized messages from accounts, or be used for cryptocurrency mining; security disruption that the antivirus software or windows updates may be disabled, preventing fixing the issue (Khan, 2012); hardware malfunction that peripheral devices like printers, keyboards, or mice may behave erratically; and unusual behavior, such that the new, unwanted files, programs, or desktop icons appear on the computer (Joshi & Patil, 2013).

6.5 Disguise

Computer viruses disguise themselves as legitimate files, software, or harmless media to evade detection and trick users into executing them (Mohajan, 2025d). They can disguise themselves before they are noticed by their side-effects. In order to stay far from the anti-virus scanners, computer viruses gradually improve their codes to make them invisible (Rad et al., 2011). There are two methods of disguise: encryption and interrupt interception. The threats of disguise can appear as invoices, reports, or documents, but are actually executable files or malicious containers designed to compromise systems (Aycock, 2006). Encryption is practically the most primitive approach to take cover the operation of the virus code that is the change of the virus body binary codes with some encryption algorithms to hide it from simple view and make it more difficult to analyze and detect. The first encrypting virus, CASCADE, appeared in 1988 (Rad et al., 2012). If the encryption method is failed, the oligomorphic viruses are willing to substitute the decryptor code in new offspring that makes the detection

process more difficult for signature based scanning engines. If the encryption and oligomorphism are faced difficulties to protect the anti-virus, polymorphism is developed that has capability to create infinite new decryptors (Szor & Ferrie, 2001). If polymorphism is failed, metamorphic virus is developed to create a new instance, which is not encrypted and does not require decryptor (Jordan, 2002).

7. Types of Computer Viruses

A computer virus is a small piece of code hidden inside a normal program. It can make copies of itself and infect other programs (Mohajan, 2025e). It can damage the system by changing or deleting files and may cause the computer to crash or not work properly (Sarkar, 2018). A virus dropper, usually a Trojan horse, helps put the virus into the computer. When the computer turns on, this virus loads into memory before the operating system starts. It can spread through infected devices like hard drives or USB drives (Wang et al., 2018). We can classify the viruses according to their origin, types of operating system attack, and their techniques of attack, what type of files they infect, how they damage, etc. (Choudhary et al., 2013). There are many types of computer viruses, and in this study, we have discussed mainly nine types of computer viruses as follows:

7.1 Boot Sector Virus

A boot sector virus is a type of virus that infects the part of a storage device and helps to start the computer, called the master boot record (MBR). It is characterized by the fact that it physically resides in the boot sector of the disk rather than in a program file (Kim et al., 2022). It is typically 512 bytes of data on personal computer (PC) that infects the boot sector of a hard disk, a floppy disk, and a pen drive by inserting itself into the boot sector of the disk (Sarkar, 2018). Most of the boot sector consists of a simple and small program that is used to start Disk Operating System (DOS), or whatever operating system is installed. When a computer is booted, the microprocessor first reads the MBR from the disk (Mohajan, 2026a). It is one of the most dangerous viruses, because it infects the MBR, notoriously difficult to remove, and requires a full system format. It is sometimes referred to as memory resident virus because it stays active in the system's memory after execution (Kumar, 2024).

The computer drive has a sector solely responsible for pointing to the operating system so that it can boot into the interface (Mishra, 2012a). The virus is loaded soon after the power on self-test and controls the system through the transferring code and remains in control at all times. It replaces the original boot sector with its own modified version. Once entered it alters the boot sector of the hard disk and remains in the hard disk permanently (Rodionov et al., 2014). It stays in the memory until the system is shut off and the disk is reformatted. Once the virus is loaded, it automatically transfers control to the area where the boot record is available (Aycock, 2006). It overwrites the original boot record with the infected one. It damages or controls the boot sector on the drive, rendering the machine unusable. When other disks are used on the infected computer, the virus is also transferred to their boot sectors (Gole, 2024).

7.2 Spyware

Spyware is a type of malware that is installed on computers and gathers information about the users and stores every keystroke that a user enters without his knowledge. It is designed to monitor computer, and tracks every online and offline activity. It can change web browser's home page or add additional components in the wave page (Kim & Solomon, 2010). It secretly monitors the users' activities and collects information, such as their net surfing habits, types of websites they visit, etc. It records and sends the collected information to advertisers or other interesting parties (Gole, 2024). It is deemed a big danger to the privacy and secrecy of both individuals and organizations. The collected data can also be used to track and capture credit card or bank account information, login and password information or user's personal identity (Wang et al., 2018). Sometimes, it changes certain computer settings which make the computer slow and difficult to work properly. Spyware detection techniques have been presented using three approaches; signature-based, behavior-based, and specification-based (Sheta et al., 2016).

7.3 Macro Virus

A "macro" is a series of instructions, such as menu selections, keystrokes, and commands that are recorded and can be played back with a single command or a keyboard stroke. It is generally triggered by pressing the key or by calling the macro name (Mishra, 2012b). A macro virus is programmed in scripting languages and generally infects document files, such as Microsoft Office Documents, Excel, and similar files without the user's knowledge (Abu & Alta,

2016). It is written in macro languages, such as Visual Basic for Applications (VBA) that is embedded inside a software application, and is relatively easy to learn. Hence, a large number of new macro viruses are created on every day (Singh & Sharma, 2017).

The macro virus resides in macros and use "macro instructions" to perform unintended and sometimes damaging actions. It delivers a payload when the file is opened and the macro runs, and infects data files. It attaches itself to a word processing or a spreadsheet file as a macro (Bontchev, 1996). When an infected document is opened, it can infect all the subsequent documents. It also spreads to other computers on transferring infected documents to those computers. It is easy to create but difficult to detect (Kumar, 2024). In 1999, a macro virus, "Melissa virus" rapidly spread to millions of computer systems worldwide that caused $10 million lost productivity and snarling computer networks with large volumes of email traffic (Mishra, 2012b).

7.4 Polymorphic Virus

A polymorphic virus is a type of malicious software that malware authors hide the malicious code via encryption and can use polymorphic code and signature each time they infect a new system to change the program's footprint to avoid detection (Gole, 2024). It is very complex virus, and after infecting a system it encrypts 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 (Choudhary et al., 2013). It has hundreds and thousands of variants. It makes many traditional cyber security tools, such as antivirus or antimalware solutions that rely on signature based detection, and fail to recognize and block the threat (Hamid et al., 2018). It controls the computer, and then decrypts the virus body, and a mutation engine generates randomized decryption routines that changes each time a virus infects a new program. Therefore, it is more difficult for an antivirus to detect and remove them (Tabary, 2011). When polymorphic viruses run, first they decrypt themselves and then behave like any other virus. For example, the "Nuke Encryption Device" (NED) and the "Trident Polymorphic Engine" (TPE) have been written that turn a standard virus into a polymorphic virus (Kumar, 2024). These viruses are the most complex and difficult to detect, often requiring anti-virus companies to spend days or months creating the detection routines needed to catch a single polymorphic. Some polymorphic viruses are Elkern, Marburg, Satan Bug, Tuarey, etc. (Chaumette et al., 2011).

7.5 Multipartite Virus

Multipartite computer viruses infect and spread through multiple methods at the same time, such as executable files and boot sectors, requiring complete removal of all parts for cleanup (Sulianta, 2022). They are fast moving and dual personality viruses and spread in multiple ways at the same time and may create a risk of cyber threats (Hasan et al., 2019). They take different actions on an infected computer depending on variables, such as the operating system installed or the existence of certain files (Sung et al., 2014). These spread across a network by copying themselves or injecting code into critical computer resources. They can simultaneously infect both the boot sector and executable files, allowing them to act quickly and spread fast (Kaur, 2019). Once the PC has been booted from an infected MBR, the virus goes memory resident and infects all accessed, EXE files. If this virus is left undetected, becomes severe threats on the computer system (Kumar, 2024).

7.6 Direct Action Virus

A direct action virus is a type of non-resident computer malware that attaches itself to specific executable files, such as .exe or .com that are specifically designed to perform a destructive activity on system. It can take direct action when a specific condition is met (Salunke & Wadhai, 2022). It can remain dormant until a specific action is taken or a timeframe passes. It stays into the root directory that is located in the hard disk and can take action at the time of booting. It is considered "non-resident", and it does not install itself or remain hidden in the computer memory (Asaad, 2020). It may be a code authored and can get installed in the memory. When a device user plans to execute a harmless file attached to the malicious code, it instantly delivers a payload. It works by attaching itself to a particular type of file. When someone executes the file, it springs into life, looking for other similar files in the directory for spreading (Choudhary et al., 2013).

7.7 Resident Virus

A resident computer virus is a type of malicious software that installs itself into the RAM of computer rather than just executing and closing, and sit dormant until a payload is delivered. As it resides in memory, it is harder to detect and

remove compared to direct-action viruses (Filiol, 2005). It can install itself somewhere in memory, and makes arrangements for the virus body in memory to be executed at some future time (Gajbe, 2020). It is one of the most harmful computer viruses, because it can penetrate any file examined by antivirus tools (Horton & Seberry, 1997).

7.8 Web Scripting Virus

A web scripting virus is malicious software that is designed to breach web browser security and executes harmful code locally on devices (Mohajan, 2026b). 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. When the virus breaches the web browser security, it injects some malicious codes to take over the web browser and alter some settings (Addison, 1999). It is among the most prevalent threat that users and organizations face. It can capture sensitive information of the device, such as usernames, passwords, and even financial details from unsuspecting users without their knowledge. When any user gives username and password then the interceptor frame hijack all the information about the user. This type of virus is able to propagate faster than any other viruses. There are two types of web scripting virus: persistent and non-persistent web scripting viruses (Szor, 2005). A persistent web scripting virus occurs when malicious code is permanently stored on a website that has the capacity to impersonate the user and cause a lot of damage. A non-persistent web scripting virus occurs when malicious code is not stored on the server. It is often used in phishing schemes and depends on immediate user interaction (Sharp, 2007).

7.9 Browser Hijacker

Browser hijacking is a severe form of cybercrime that affects internet browsers worldwide. It is a malware program that can sneak onto the device through freeware, adware, or spyware. It is the act of altering a user web browser setting without the consent of a user that results in detrimental effects on the privacy and security of a user (Patil & Dash, 2024). It can cause mild disorder to severe threat, and a user can experience inconveniences of facing identity theft that results steal of usernames, passwords, credit cards, and other important information (Zonta & Sathiyanarayanan, 2024). There are a number of browser hijackers, such as Astromenda, Ask Toolbar, Mindspark, Dregol, Binkiland, ESurf, Groovorio, Delta and Claro, Sweet Page, Jamenize, Mazy Search, etc. A browser hijacker may replace the existing home page, error page, or search engine with its own (Singh, 2017). Browser hijackers are developing various trusted brands to cover up their malicious intentions, and such kind of attacks can be avoided by not installing plugins from unknown sources, keeping browser patches up to date, installing antivirus software, taking precautions when downloading software, etc. (Kumar & Indrani, 2018).

7.10 File Infector Virus

A file infector virus is a classic type of malware that attaches itself directly into legitimate executable files, such as .exe, .bat, .dll or .com files and can be dangerous for any device. It can be spread with the help of games and word processors. It is completely self-executive and can make multiple copies of the file itself (Mishra, 2013). It can cause permanent damage to the device. When the infected file is run, the virus becomes active and can spread by infecting other executable files on the system by attaching itself to the end of a file (Morales et al., 2010). It spreads in a device faster, and it is enough to destroy the whole device's workability. It changes the start of a program so that the control jumps to its code (Russell & Gangemi, 1991). It usually transfers control back to the original program, making the infection less noticeable. It is also known as parasitic virus, because it depends on host files to function but keeps the host operational (Kabulov et al., 2020).

7.11 Overwriting Virus

An overwriting virus is a highly destructive malware that targets .exe or .com computer files and changes the original code of an executable program, and then replaces it with malicious code or deletes it (Daoud, 2008). In this situation, the recovering of the original data is almost impossible. It is extremely harmful because it completely destroys elements of a user's system (Maity & Dey, 2021). It is considered as the most harmful virus, because it affects the original code and removes the existing program. Some overwriting viruses are Yankee Doodle, Way, Trj.Reboot, Trivial.88.D, Gorg.202/456, Gorj.377, Loveletter, etc. (Choudhary et al., 2013).

8. Parts of Computer Viruses

A computer virus is a very small portion of a program that can attach itself to another program

within the computer, and spreads among computers, and damages data and software. It generally contains three parts: i) the infection mechanism, which finds and infects new files, ii) the payload, which is the malicious code to execute, and iii) the trigger, which determines to activate the payload (Stallings, 2012).

8.1 Infection Mechanism

Computer virus infection mechanisms refer to the processes by which malicious software replicates, hides, and spreads to other files, programs, and computer systems. It is also called the infection vector that has the specific paths or methods, and a computer virus uses these to penetrate a system and spreads its malicious payload through some vulnerability (Şcheau et al., 2015). It differs depending on the used transmission channel and the targets victim. Some viruses have a search routine, which locate and infect files on disk. Other viruses infect files as they run, such as the Jerusalem DOS virus (Filiol, 2005). When the user executes the infected file, the virus activates, replicates itself by modifying other files, and spreads to new systems via networks, shared drives, or email attachments (Zimba, 2017).

8.2 The Trigger

The trigger is also known as a logic bomb, and a time-based trigger is often called a time bomb. It is the part of the virus that determines the condition for which the payload is activated. It is a hidden and unauthorized piece of malicious code that embedded in an application or network (Dusane & Pavithra, 2020). It lies dormant until a specific and predetermined condition is met. It can be positive, when an action occurs, or negative, when an action does not occur. It may happen in a particular date, time, event-based, user actions, size on disk exceeding a threshold, system conditions, presence of other program, and opening a specific file (Bist, 2014). It executes its payload, causing damage to the targeted system when the trigger is activated. The purpose of trigger is to cause harm, disrupt operations, delete or corrupt data, or steal sensitive information (Sharma, 2017).

8.3 Payload

A payload in computing refers to the essential data, message, and files being transmitted through the malicious code executed after a system is breached. It is the body of the virus that executes the malicious activity, such as damaging files, theft of confidential information or spying on the infected system, either intentional or accidental (Farrukh et al., 2022). Accidental damage may result from bugs in the virus, encountering an unknown type of system, or perhaps unanticipated multiple viral infections. Headers and metadata are sent only to enable payload delivery and are considered overhead (Almansour & Mustafa, 2014). Payload activity is sometimes noticeable as it can cause the system to slow down or "freeze". Sometimes payloads are non-destructive and spread a message to as many people as possible, which is called a virus hoax (Wang et al., 2018).

9. Protection System from Virus Attacks

Computer viruses can be easily spread through the emails, email attachments, internet downloads, visiting unknown web pages, installing unknown software, etc. Unwitting users can be victim of hacking easily (Polk et al., 1995). When a computer is infected with viruses, it will show different odd symptoms of its activities, such as it will start to slow down without any reason, abruptly restart itself, often new shortcuts or other icons will be seen in the computer that are not created by the user, visible of unusual error messages and display abnormal behavior, applications installed on the computer will not function as expected (Zhang, 2022). Some files may be deleted of without the permission of the user, etc. It is a good practice to follow some simple precautionary measures that can reduce the possibility of a virus attack (Khan et al., 2017).

Computer virus protection depends on a combination of genuine antivirus software, safe browsing habits, and system updates (Arinze & Agwu, 2024). Anti-virus software is also known as anti-malware and is a computer program that identifies, detects, prevents, inoculates, and takes action to disarm or remove malicious software, such as viruses and worms (Cohen, 1984). It helps users against the latest virus threats. It scans all the files and folders of the computer system to look for the viruses listed in its database of viruses. It removes the virus and repairs the infected file (Zhu et al., 2012).

At present there are a lot of anti-virus software product companies. Some popular antivirus programs are Norton antivirus software, Backdoor antivirus, McAfee virus scan, AVG antivirus, Avast antivirus, Panda antivirus, Dr. Solomon antivirus toolkit, Web scan antivirus, Kaspersky antivirus, Trend Micro antivirus, Avira antivirus, Logic Bomb antivirus, Rabbit

antivirus, Bitdefender antivirus, Smadav antivirus, Symantec antivirus, ESET, HTTP (Hyper Text Transfer Protocol), Thunder byte antivirus, Comodo antivirus, Sophos antivirus, Firewall antivirus, F-secure antivirus, USB disk security, Microsoft Security Essentials, McAfee, Malwarebytes, etc. (Coulthard & Vuori, 2002; Filiol et al., 2007).

10. Conclusions

Computer viruses are instructions that are hidden within a computer program and are designed to cause faults or destroy data. They are capable of perpetuating themselves with the basic objective of performing certain activities that could range from annoyance to serious vandalism. They can spread by attaching copies of themselves to some part of a program file, such as a spreadsheet or word processor. In this study, we have studied different types of computer viruses and their characteristics, the threat faced by computer virus, and different preventive measures. If we have the detail knowledge about viruses, we can secure our system very efficiently. The computer viruses are omnipresent as like air in digital world. It passes from computer to computer like a biological virus passes from person to person. But it never occurs naturally and always induced by people. At present the use of computer in digital word is increasing day by day due to the dependency on the networking. Cybercriminals launch and spread virus over the network and steal or alter information for their own benefits. The computer viruses are causing billions of dollars worldwide each year through the economic damages. Various industries are creating, selling or freely distributing antiviruses to users of various operating systems.

References

Abdulmalik, U., I., et al. (2024). A Survey on the Effect of Computer Virus Attacks and Its Preventive Measures among Computer Users. *Kasu Journal of Computer Science, 1*(2), 134-150.

Abu, M. S., & Alta, N. M. (2016). The Rise of Macro Malware in Malaysia. *E-Security, 41*, 6-9.

Addison, C. (1999). Webwatch: Web Security Viruses and Malware. *Information Development, 15*(2), 79-82.

Almansour, S. M, E., & Mustafa, A. B. A. (2014). Effect of Payload Virus as Threatening for Internet Security. *International Journal of Modern Communication Technologies & Research, 2*(9), 39-42.

Arinze, E. D., & Agwu, C. O. (2024). Advancements in Computer Virus Protection: From Origins to Future Trends. *Eurasian Experiment Journal of Scientific and Applied Research, 6*(1), 11-16.

Arnold, W., & Tesauro, G. (2000). Automatically Generated Win32 Heuristic. Virus Bulletin Conference, September 2000.

Asaad, R. R. (2020). Implementation of a Virus with Treatment and Protection Methods. *Icontech International Journal of Surveys, Engineering, Technology, 4*(2), 28-34.

Aycock, J. (2006). *Computer Viruses and Malware*. Publisher: Springer, Canada.

Bhome, S., et al. (2013). *Research Methodology*. Himalaya Publishing House, New Delhi.

Bist, A. S. (2014). Detection of Logic Bombs. (*International Journal of Engineering Sciences & Research, 3*2), 777-779.

Bontchev, V. (1996). Possible Macro Virus Attacks and How to Prevent Them. *Computers & Security, 15*(7), 595-626.

Burger, R. (1991). *Computer Viruses and Data Protection*. Grand Rapids, MI: Abacus.

Chaumette, S., et al. (2011). Automated Extraction of Polymorphic Virus Signatures using Abstract Interpretation. Proceedings of the 5th International Conference on Network and System Security, Milan, Italy.

Choudhary, S., et al. (2013). Awareness about Viruses. *International Journal of Emerging Research in Management &Technology, 2*(4), 42-45.

Cohen, F. (1984). Computer Viruses: Theory and Experiments. *Computers & Security, 6*(1), 22-35.

Coulthard A., & Vuori, T. A. (2002). Computer Viruses: A Quantitative Analysis. *Logistics Information Management, 15*(5/6), 400-409.

Creswell, J. W. (2013). *Research Design: Qualitative, Quantitative, and Mixed Method Approaches* (4th Ed.). Thousand Oaks, California: SAGE Publications.

Daoud, E. A. (2008). Computer Virus Strategies and Detection Methods. *International Journal of Open Problems in Computer Science, 1*(2), 122-129.

Dixit, N. K., et al. (2012). The New Age of Computer Virus and Their Detection. *International Journal of Network Security & Its Applications, 4*(3), 79-96.

Dusane, P. S., & Pavithra, Y. (2020). Logic Bomb: An Insider Attack. *International Journal of Advanced Trends in Computer Science and Engineering, 9*(3), 3662-3665.

Farrukh, Y. A., et al. (2022). Payload-Byte: A Tool for Extracting and Labeling Packet Capture Files of Modern Network Intrusion Detection Datasets. TechRxiv.

Filiol, E. (2005). *Computer Viruses: From Theory to Applications*. Springer-Verlag, France.

Filiol, E., et al. (2007). Evaluation Methodology and Theoretical Model for Antiviral Behavioral Detection Strategies. *Journal in Computer Virology, 3*(1), 27-37.

Franklin, M. I. (2012). *Understanding Research: Coping with the Quantitative-Qualitative Divide*. London and New York: Routledge.

Gajbe, A. (2020). Computer Virus: Their Problems & Major Attacks in Real Life. *Journal of Emerging Technologies and Innovative Research, 7*(8), 652-659.

Galvan, J. L. (2015). *Writing Literature Reviews: A Guide for Students of the Social and Behavioral Sciences* (6th Ed.). Pyrczak Publishing.

Gole, D. (2024). Computer Viruses. *National Journal of Hindi & Sanskrit Research, 1*(56), 64-67.

Hamid, I. R., et al. (2018). Classification of Polymorphic Virus Based on Integrated Features. *International Journal n Advanced Science Engineering Information Technology, 8*(6), 2577-2583.

Hannah, S. (2019). Literature Review as a Research Methodology: An Overview and Guidelines. *Journal of Business Research, 104*, 333-339.

Hasan, H., et al. (2020). Enhancing Monkey to Trigger Malicious Payloads in Android Malware. Proceedings of the 17th International ISC Conference on Information Security and Cryptology.

Hasan, M. Z., et al. (2019). Computer Viruses, Attacks, and Security Methods. *LGU Research Journal for Computer Sciences & IT, 3*(3), 20-25.

Highland, H. J. (1997). A History of Computer Viruses: The Famous 'Trio'. *Computers & Security, 16*(5), 416-429.

Horton, J., & Seberry, J. (1997). Computer Viruses: An Introduction. Proceedings of the 20th Australasian Computer Science Conference, Sydney, Australia, February 5-7, 1997.

Howell, K. E. (2013). *Introduction to the Philosophy of Methodology*. London, UK: Sage Publications.

Jesdanun, A. (2007). School Prank Starts 25 Years of Security Woes. Consumer News and Business Channel (CNBC).

Jordan, M. (2002). Dealing with Metamorphism. *Virus Bulletin, 1*(10), 4-6.

Joshi, M. J., & Patil, B. V. (2013). Computer Virus: Their Problems & Major Attacks in Real Life. *International Journal of P2P Network Trends and Technology, 3*(4), 206-209.

Kabulov, A., et al. (2020). Computer Viruses and Virus Protection Problems. *Science and Education, 1*(9), 179-184.

Kara, H. (2012). *Research and Evaluation for Busy Practitioners: A Time-Saving Guide*. Bristol: The Policy Press.

Kaur, J. (2019). Taxonomy of Malware: Virus, Worms and Trojan. *International Journal of Research and Analytical Reviews, 6*(1), 192y-196y.

Kephart, J. O., & White, S. R. (1993). Measuring and Modeling Computer Virus Prevalence. Proceedings 1993 IEEE Computer Society Symposium on Research in Security and Privacy.

Khan, H. A., et al. (2017). Computer Virus and Protection Methods Using Lab Analysis. IEEE 2nd International Conference on Big Data Analysis, pp. 882-885.

Khan, I. (2012). An Introduction to Computer Viruses: Problems and Solutions. *Library Hi Tech News, 29*(7), 8-12.

Kim, D., & Solomon, M. G. (2010). *Fundamentals of Information Systems Security*. Jones & Bartlett Publishers.

Kim, T. N., et al. (2022). Detecting Malware in Portable Executable Files Using Machine Learning Approach. *International Journal of Network Security & Its Applications, 14*(3), 11-17.

Kumar, M. S., & Indrani, B. (2018). A Study on Web Hijacking Techniques and Browser

Attacks. *International Journal of Applied Engineering Research, 13*(5), 2614-2618.

Kumar, V. (2024). Computer-Virus: Types and Its Prevention. *Journal of American Science, 20*(5), 9-12.

Ludwig, M. A. (1996). *The Little Black Book of Computer Viruses: The Basic Technologies* (Volume 1). American Eagle Publications.

Maity, S., & Dey, D. (2021). Computer Virus Attacks. *Pensee International Journal, 51*(3), 585-594.

Markoff, J. (1999). Digital Fingerprints Leave Clues to Creator of Internet Virus. *The New York Times*.

Miller, G. (1996). Technology: 'Boza' Infection of Windows 95 a Boon for Makers of Antivirus Software. *Los Angeles Times*.

Mishra U. (2013). Methods of Repairing Virus Infected Files, A TRIZ based Analysis. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.2265576

Mishra, U. (2012a). Detecting Boot Sector Viruses: Applying TRIZ to Improve Anti-Virus Programs. *SSRN Electronic Journal*. http://dx.doi.org/10.2139/ssrn.1981886

Mishra, U. (2012b). Detecting Macro Viruses: A TRIZ Based Analysis. *SSRN Electronic Journal.* http://dx.doi.org/10.2139/ssrn.1981892

Mohajan, H. K. (2017). Two Criteria for Good Measurements in Research: Validity and Reliability. *Annals of Spiru Haret University Economic Series, 17*(3), 58-82.

Mohajan, H. K. (2018a). *Aspects of Mathematical Economics, Social Choice and Game Theory*. PhD Dissertation. University of Chittagong, Chittagong, Bangladesh.

Mohajan, H. K. (2018b). Qualitative Research Methodology in Social Sciences and Theoretical Economics. *Journal of Economic Development, Environment and People, 7*(1), 23-48.

Mohajan, H. K. (2020). Quantitative Research: A Successful Investigation in Natural and Social Sciences. *Journal of Economic Development, Environment and People, 9*(4), 50-79.

Mohajan, H. K. (2025a). Artificial Intelligence: Prospects and Challenges in Future Progression. *Art and Society, 4*(7), 38-50.

Mohajan, H. K. (2025b). Deep Learning: A Brief Study on Its Architectures and Applications. *Art and Society, 4*(8), 41-49.

Mohajan, H. K. (2025c). Cybercrime: A Potential Threat to Global Community. *Studies in Social Science & Humanities, 4*(6), 28-39.

Mohajan, H. K. (2025d). Vulnerability of Cyber Security is an Unexpected Threat to Global Internet System. *Art and Society, 4*(9), 1-14.

Mohajan, H. K. (2025e). Cyber Child Pornography: An Unexpected Global Heinous Crime against Children. *Art and Society, 4*(10), 7-13.

Mohajan, H. K. (2026a). Addiction and Consumption of Cyber Pornography have Increased Risk Factors and Harmful Effects among Emerging Adults. *Studies in Social Science & Humanities, 5*(1), 33-40.

Mohajan, H. K. (2026b). Machine Learning: A Brief Review for the Beginners. *Innovation in Science and Technology, 5*(1), 26-34.

Morales, J. A., et al. (2010). Identification of File Infecting Viruses through Detection of Self-Reference Replication. *Journal in Computer Virology, 6*(2), 161-180.

Oyelere, S. S., & Oyelere, L. S. (2015). Users' Perception of the Effects of Viruses on Computer Systems: An Empirical Research. *African Journal of Computing & ICT, 8*(1), 121-130.

Parikka, J. (2007). Digital Contagions: A Media Archaeology of Computer Viruses. New York: Peter Lang.

Patil, S., & Dash, C. A. (2024). Effective Detection and Mitigation of Browser Hijacking Using Deep Learning Models. *International Journal of Multidisciplinary Research, 6*(5), 14.

Polk, W. T., et al. (1995). *Antivirus Tools and Techniques for Computer Systems*. William Andrew.

Rad, B. B., et al. (2011). Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey. *International Journal of Computer Science Issues, 8*(1), 113-121.

Rad, B. B., et al. (2012). Camouflage in Malware: From Encryption to Metamorphism. *International Journal of Computer Science and Network Security, 12*(8), 74-83.

Rajesh, D., et al. (2019). Malwares: Creation and

Avoidance. *International Journal of Computer Sciences and Engineering, 7*(4), 179-183.

Rocco, T. S., et al. (2011). *The Handbook of Scholarly Writing and Publishing*. San Francisco, CA: John Wiley & Sons.

Rodionov, E., et al. (2014). Bootkits: Past, Present & Future. Virus Bulletin Conference, September 2014, pp. 319-326.

Roffee, J., & Waling, A. (2016). Resolving Ethical Challenges When Researching with Minority and Vulnerable Populations: LGBTIQ Victims of Violence, Harassment and Bullying. *Research Ethics, 13*(1), 4-22.

Russell, D., & Gangemi, G. T. (1991). *Computer Security Basics*. O'Reilly.

Salunke, S., & Wadhai, S. A. (2022). Computer Virus and Security. *International Journal of Advanced Research in Computer and Communication Engineering, 11*(4), 754-759.

Sarkar, L. H. (2018). Computer Virus. *International Journal of Creative Research Thoughts, 6*(2), 260-261.

Sayama, H. (2006). Self-Replicating Machines Attempting to Solve the Unsolvable. Workshop on Machine Self-Replication, Tenth International Conference on the Simulation and Synthesis of Living Systems (ALife X).

Şcheau, M. C., et al. (2015). Infection Vectors: Risk Factors for Financial Transactions. *International Journal of Information Security and Cybercrime, 4*(2), 73-85.

Sharma, B. (2017). A Pragmatic Way of Logic Bomb Attack Detection Methodology. *Indian Journal of Science and Technology, 10*(20), 1-5.

Sharp, R. (2007). *An Introduction to Malware*. DTU Library.

Sheta, M. A., et al. (2016). Spyware Detection by Extracting and Selecting Features in Executable Files. Proceedings of the 10th International Conference on Electrical Engineering ICEENG 19-21 April, 2016.

Singh, I., & Sharma, S. (2017). Proposing OMVDPM: Offline Macro Virus Detection and Prevention Mechanism. *International Journal of Computer Applications, 170*(3), 19-22.

Singh, S. (2017). Browser Hijacking: Reasons and Solution. *International Journal for Innovative Research in Multidisciplinary Field, 3*(10), 166-167.

Stallings, W. (2012). *Computer Security: Principles and Practice*. Boston: Pearson.

Sulianta, F. (2022). Comparison of the Computer Viruses from Time to Time. *Central Asia and the Caucasus, 23*(1), 1386-1391.

Sung, P., et al. (2014). Understanding the Propagation Dynamics of Multipartite Computer Virus. *Industrial Management & Data Systems, 114*(1), 86-106.

Szor, P. (2005). *The Art of Computer Virus: Research and Defense*. Publisher: Linda McCarthy.

Szor, P., & Ferrie, P. (2001). Hunting for Metamorphic. *Virus*, 123-143.

Tabary, R. (2011). Context-Free Signatures for Some in-the-wild Polymorphic Viruses. [Online]. Available: www.labri.fr/perso/tabary/publis/polysigns.pdf

Torraco, R. J. (2016). Writing Integrative Literature Reviews: Using the Past and Present to Explore the Future. *Human Resource Development Review, 15*(4), 404-428.

von Neumann, J. (1966). *Theory of Self-Reproducing Automata: Essays on Cellular Automata*. University of Illinois Press.

Wang, J., et al. (2018). The Computer Network Security and Preventive Measures in the Background of Big Data Era. *Advances in Engineering Research*, 137, 413-417.

Yoo, I. (2004). Visualizing Windows Executable Viruses Using Self-Organizing Maps. *Proceedings of the 2004 ACM Workshop on Visualization and Data Mining for Computer Security*, pp. 82-89. 29 October 2004, Washington DC, USA.

Zeidanloo, H. R., et al. (2010). All about Malwares (Malicious Codes). Proceedings of the 2010 International Conference on Security & Management, SAM 2010, July 12-15, 2010, Las Vegas Nevada, USA, 2 Volumes.

Zhang, N. (2022). Computer Virus and Anti-Virus Technology. 3rd International Conference on Language, Art and Cultural Exchange. *Advances in Social Science, Education and Humanities Research*, pp. 91-103, Atlantis Press.

Zhu, Q. et al. (2012). Modeling and Analysis of the Spread of Computer Virus. *Communications in Nonlinear Science and Numerical Simulation, 17*(12), 5117-5124.

Zimba, A. (2017). Malware-Free Intrusion: A Novel Approach to Ransomware Infection Vectors. *International Journal of Computer Science and Information Security, 15*(2), 317-325.

Zonta, T., & Sathiyanarayanan, M. (2024). A Holistic Review on Detection of Malicious Browser Extensions and Links using Deep Learning. In 2024 IEEE 3rd International Conference on AI in Cybersecurity (ICAIC) (pp. 1-6). IEEE.