IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

# A Report on Hazards of Computer Viruses

**Vicky Kumawat and Varun Kumar**
Student, Master of Computer Application
Late Bhausaheb Hiray S.S Trust's Hiray Institute of Computer Application, Mumbai, India

**Abstract:** *Computer viruses are one of the major risks that an individual and a community face to the safe living of a household, enterprise, and government. These malicious software programs are developed to work like viruses: they reproduce themselves and spread, thus damaging the system, data loss and the loss of money. This research paper focuses on the various types of dangers that computer viruses pose, such as data corruption, theft of personal information, system disruption, and reputational damage. The hazards of computer viruses are the main thing that people and organizations need to be aware of in order to protect themselves and their systems from these hazards.*

*Furthermore, computer viruses can also steal sensitive information, such as passwords, credit card numbers, and personal documents. This theft of personal information can result in financial loss and identity theft. Additionally, viruses can cause system damage, leading to system crashes or malfunctions. This can disrupt normal operations and lead to costly repairs or replacements.*

**Keywords**: Identity Theft, Malicious Software, Data Corruption

## I. INTRODUCTION

Computer viruses are a prevalent threat in the digital era, posing significant risks to personal and organizational data security. These malicious programs are designed to replicate themselves and spread across computer systems, often causing various degrees of damage. The term "computer virus" was first coined in the 1980s, reflecting the way these programs infect systems similarly to how biological viruses infect living organisms. One of the primary risks associated with computer viruses is data loss and corruption. Viruses can delete or alter files, leading to the loss of critical information such as personal documents, financial records, and proprietary business data. Additionally, some viruses are engineered to steal sensitive information like passwords, credit card details, and personal identification numbers, resulting in identity theft and financial fraud. The damage caused by these viruses can disrupt normal operations, leading to costly system repairs and operational downtime.

Beyond the direct impact on data and systems, computer viruses can cause extensive network disruption and reputational damage. As viruses spread across networks, they can compromise multiple systems, causing widespread operational issues and significant downtime for businesses and organizations. This leads to lost productivity and revenue and can tarnish the affected entities' reputations. Customers and partners may lose trust in a company's ability to protect their data, resulting in long-term reputational harm. To mitigate these risks, it is essential to implement robust security measures, including regularly updated antivirus software, safe browsing practices, and comprehensive data backup strategies. Understanding the risks posed by computer viruses and taking proactive steps to address them is crucial for maintaining the security and integrity of digital systems. Today enterprise networks are distributed to different geographical locations and applications are more centrally located. Every company's data is the most valuable asset and must be treated as such. With the growing number of harmful threats; such as Viruses, Spyware, and Hackers, it has become mandatory to protect yourself against them. The most powerful way for communication and data transfer is the internet because the Internet's speed increases daily. People can transfer large amounts of data within a few minutes from one location to another location worldwide. Computers are used extensively to process data and to provide information for decision making therefore it is necessary to control their use. Due to the organizational cost of data loss, the cost of incorrect decision-making, and the value of computer software hardware organizations suffer a major loss therefore the integrity of data and information must be maintained.

This report aims to provide a comprehensive overview of the history, evolution, and notable examples of computer viruses. It explores the different types of viruses, their methods of infection, and the impact they have had on computer

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

systems and networks. Additionally, the report discusses future trends and challenges regarding computer viruses, including the increasing sophistication of malware, and the rise of AI and machine learning in cyberattacks.

## II. HISTORY OF COMPUTER VIRUSES

**Early Concepts and First Viruses (1970s-1980s)**

- **The Creeper Virus (1971):** Considered the first computer virus, created by Bob Thomas. It was a self-replicating program that infected DEC PDP-10 mainframes running the TENEX operating system. Creeper displayed the message, "I'm the creeper, catch me if you can!"
- **Elk Cloner (1982):** One of the first known viruses to spread in the wild, created by a high school student named Rich Skrenta. It infected Apple II systems via floppy disks, displaying a poem after the 50th boot.
- **Brain (1986):** Created by Pakistani brothers Amjad and Basit Farooq Alvi, Brain is often cited as the first PC virus. It targeted the boot sector of MS-DOS systems.

**Emergence of Polymorphic and Macro Viruses (1990s)**

- **Polymorphic Viruses:** These viruses can change their code to evade detection by antivirus software. The first widely known polymorphic virus was **The Chameleon Virus** (1990).
- **Concept Virus (1995):**The first macro virus, Concept, targeted Microsoft Word documents. It demonstrated the potential of exploiting macro-scripting languages to spread malware.

**Widespread Internet and Email Viruses (Late 1990s-2000s)**

- **Melissa Virus (1999):** Spread via infected email attachments, Melissa caused widespread disruption by sending itself to the first 50 contacts in the victim's email address book.
- **ILOVEYOU Virus (2000):** Another email-based virus, ILOVEYOU, caused significant damage by tricking users into opening an attachment disguised as a love letter. It affected millions of computers worldwide.

**Worms and Network-Based Viruses (2000s)**

- **Code Red (2001):** A worm that targeted vulnerabilities in Microsoft IIS web servers, infecting over 359,000 hosts in less than 14 hours.
- **Nimda (2001):** A highly sophisticated worm that spread through multiple vectors, including email, open network shares, and web servers. It caused extensive damage and network congestion.

**Ransomware and Advanced Persistent Threats (APTs) (2010s-Present)**

- **CryptoLocker (2013):** Marked the rise of ransomware, encrypting victims' files and demanding payment in Bitcoin for the decryption key.
- **WannaCry (2017):** A ransomware attack that exploited a Windows vulnerability to spread rapidly across the globe, affecting critical infrastructure and businesses.
- **SolarWinds (2020):** An APT that compromised the software supply chain, inserting a backdoor into the Orion software used by numerous government agencies and large enterprises.

**Evolution of Virus Types and Their Sophistication**

- Boot Sector Viruses (1980s)
- Targeted the master boot record of disks.
- Spread through infected floppy disks and later USB drives.

**File Infectors (1980s-1990s)**

- Attached themselves to executable files.
- Activated when the infected file was executed.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

**Polymorphic Viruses (1990s)**

- Changed their code with each infection to avoid detection.
- Required advanced detection techniques from antivirus software.

**Macro Viruses (1990s)**

- Exploited macro languages in office applications.
- Spread through infected documents and spreadsheets.

**Worms (Late 1990s-2000s)**

- Self-replicating and spread through networks.
- Examples include Code Red and Nimda.

**Ransomware (2010s-Present)**

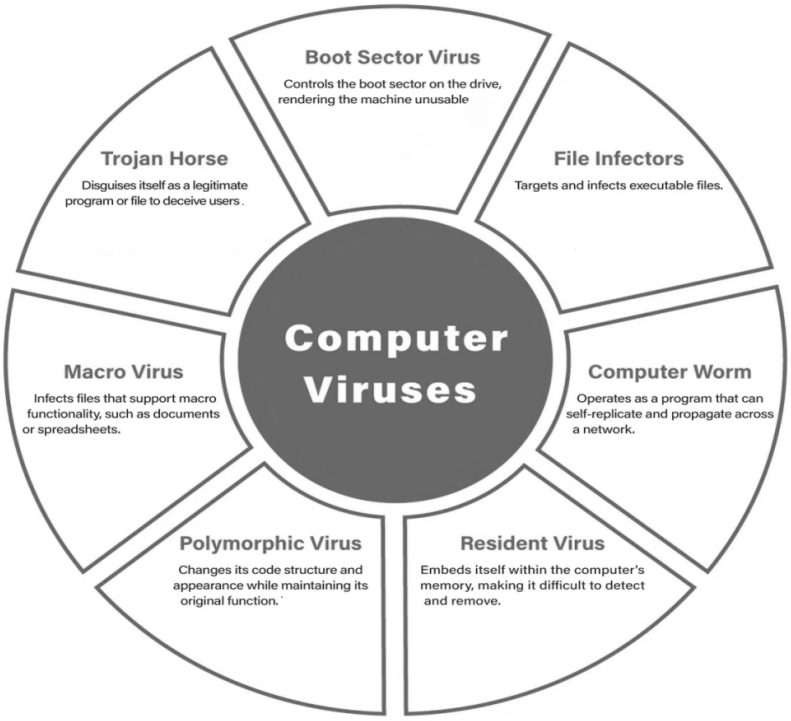
- Encrypted victims' files and demanded ransom for decryption.
- Evolved to include double extortion tactics, threatening to release stolen data.

**Advanced Persistent Threats (APTs) (2010s-Present)**

- Highly sophisticated attacks are often linked to nation-state actors.
- Focused on long-term espionage and data theft.

## III. DIFFERENT TYPES OF VIRUSES

Computer viruses are malicious software programs designed to infect and manipulate systems without the user's consent. They come in various forms, each with distinct characteristics and methods of operation.




Here are some common types of computer viruses and a brief explanation of how they work:

**Boot Sector Viruses**

**Description:**

- Infect the master boot record (MBR) of a hard disk or removable storage device.
- Activate when the system is booted from the infected drive.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

**How they work:**

- Load into memory during the boot process and can infect other disks.
- IT is often spread through infected floppy disks or USB drives.
- Impact: Can render a system unbootable, causing significant disruption and requiring specialized tools to remove.

**File Infectors**

**Description:**

- Attach themselves to executable files (.exe, .com, etc.).

**How they work:**

- Activate when the infected file is executed.
- It can be replicated by attaching to other executable files.
- Impact: Can corrupt or delete files, leading to data loss and system instability.

**Trojan Horses**

**Description:**

- It is disguised as legitimate software but contains malicious code.

**How they work:**

- Users are tricked into installing them, thinking they are legitimate.
- Once installed, they can execute harmful actions such as stealing data or creating backdoors.
- Impact: Can compromise system security, leading to unauthorized access and potential data breaches.

**Macro Viruses**

**Description:**

- Written in the macro language of applications like Microsoft Word or Excel.

**How they work:**

- Spread through infected documents or spreadsheets.
- Activate when the infected document is opened, potentially infecting other documents.
- Impact: Can cause widespread infection across an organization by exploiting commonly used office documents.

**Computer Worms**

**Description:**

- Self-replicating malware that spreads without user intervention..

**How they work:**

- Exploit network vulnerabilities to spread to other computers.
- Can consume bandwidth and overload systems, leading to denial-of-service (DoS) attacks.
- Impact: Can cause significant network disruption and slow down or crash entire networks.

**Polymorphic Viruses**

**Description:**

- Change their code or signature patterns to avoid detection.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

**How they work:**

- Use encryption or obfuscation techniques to alter their appearance with each infection.
- Makes it challenging for antivirus software to detect them.
- Impact: Prolong the duration and spread of an infection, making eradication difficult.

**Resident Viruses**

**Description:**

- Embed themselves in the computer's memory.

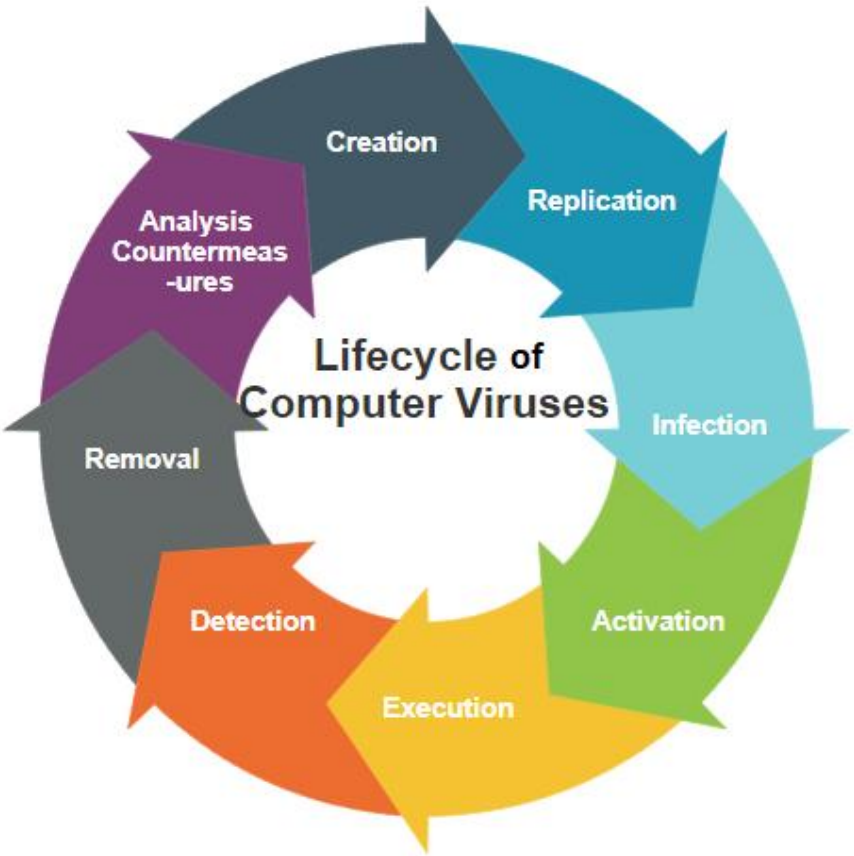
**How they work:**

- Can execute any time the operating system is running.
- Infect other files and programs by remaining active in memory.
- Impact: Can continuously infect new files and applications, leading to persistent system issues and degradation.

These types of viruses all have unique characteristics and different ways of spreading, making it difficult to detect them and eliminate them.

## IV. LIFE CYCLE OF COMPUTER VIRUSES

The life cycle of a computer virus encompasses several critical stages, from its inception and spread to its eventual detection and eradication, each playing a vital role in the impact and persistence of the malware, which is as follows :



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

**Creation**

The life cycle of a computer virus begins with its creation. A programmer or hacker writes the virus using a programming language, often with a specific intent such as theft, espionage, disruption, or simply causing chaos. The creator designs the virus to exploit specific vulnerabilities, spread in certain ways, and execute a predefined payload. This stage involves considerable planning and coding, ensuring the virus can evade detection and achieve its goals.

**Replication**

Once the virus is created, it enters the replication phase. The virus begins to reproduce itself, either immediately or when triggered by certain conditions. Replication involves the virus attaching itself to executable files, or documents, or spreading through network connections and removable media like USB drives. The virus might also exploit network protocols to move between systems without user interaction. The goal of replication is to maximize the number of infected systems, increasing the virus's reach and potential impact.

**Infection**

The next stage is infection, where the virus infiltrates a host system. It embeds itself into files or memory, becoming part of the system's regular operations. This can involve modifying or overwriting files, exploiting system vulnerabilities, or executing malicious code when an infected file is opened. During this stage, the virus can remain dormant or active, depending on its design. Infection allows the virus to establish a foothold in the system, setting the stage for further actions.

**Activation**

In the activation stage, the virus's payload—the part of the virus that performs the malicious action—is triggered. Activation can be based on specific events, such as a particular date, user actions (like opening an infected file), or reaching a certain number of infections. For example, some viruses are designed to activate on April 1st, while others might activate after infecting 100 systems. This stage is crucial as it determines when and how the virus will execute its malicious activities.

**Execution**

Once activated, the virus enters the execution stage, carrying out its malicious payload. This can include a wide range of harmful activities, such as corrupting or deleting data, stealing information (like passwords or credit card numbers), creating backdoors for unauthorized access, displaying unwanted messages, or disrupting system operations. The effects of these actions can vary from minor annoyances to severe damage and data loss, depending on the virus's design and intent.

**Detection**

Eventually, the virus is detected in the detection stage. Security software or IT professionals identify the presence of the virus, typically through antivirus scans, unusual system behavior, or network monitoring. Detection can also occur through user reports of strange activities or system performance issues. Modern antivirus programs use signature-based detection, heuristic analysis, and behavioral monitoring to identify viruses. Once detected, the focus shifts to containment and eradication.

**Removal**

Upon detection, the system enters the removal stage, where efforts are made to eliminate the virus. This can involve using antivirus software to scan and remove infected files, manual removal procedures for more stubborn infections, system restoration from backups, or, in severe cases, reinstalling the operating system to ensure complete eradication. Effective removal is critical to restoring system functionality and preventing further spread of the virus.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

**Analysis and Countermeasures**

Following removal, the analysis and countermeasures stage occurs. Security experts analyze the virus to understand its behavior, origin, and impact. This analysis helps in developing virus signatures for detection, creating patches to fix vulnerabilities, and improving security protocols to prevent future infections. For instance, they might update antivirus definitions, enhance firewall rules, and educate users on safe practices. This stage also involves incident response to assess damage and restore normal operations.

By understanding the life cycle of a computer virus, individuals and organizations can implement effective strategies to prevent infections, detect viruses early, and mitigate their impact on systems and networks. This comprehensive approach ensures a robust defense against the evolving threat landscape posed by computer viruses.

## V. COMPUTER VIRUS ATTACKS

In recent years, several computer viruses and malware attacks have gained significant attention due to their widespread impact and sophisticated methods. One of the most notorious attacks was WannaCry in 2017, a ransomware that exploited a vulnerability in the Windows operating system known as EternalBlue. WannaCry affected hundreds of thousands of computers in over 150 countries, encrypting files on infected systems and demanding ransom payments in Bitcoin. The attack notably disrupted healthcare organizations, including the UK's National Health Service (NHS), causing significant operational disruptions.

Another major attack in 2017 was NotPetya, initially appearing as ransomware but later identified as a wiper, designed to irreversibly damage data. NotPetya spread through a compromised update of the Ukrainian accounting software MeDoc, causing substantial damage to major companies such as Maersk, Merck, and FedEx, leading to billions of dollars in losses.

Emotet, active from 2018 to 2021, started as a banking Trojan and evolved into a highly modular malware distribution platform. It spread primarily through malicious email attachments and links and was used to deliver other malware, including ransomware like Ryuk and TrickBot. Emotet was eventually disrupted by a coordinated international law enforcement effort in January 2021.

Ryuk, another ransomware that emerged in 2018, targeted large organizations and demanded high ransom payments. Often used in conjunction with other malware such as Emotet and TrickBot, Ryuk was responsible for attacks on various sectors, including healthcare, government, and education, leading to significant operational disruptions and financial losses.

In 2019, Maze ransomware became known for its double extortion tactic, where attackers not only encrypted data but also threatened to publish it unless a ransom was paid. Maze targeted a wide range of industries, including IT, healthcare, and finance. Although the group disbanded in late 2020, its techniques have been adopted by other ransomware groups.

One of the most sophisticated and widespread cyber-espionage campaigns was the SolarWinds attack in 2020. This supply chain attack involved the compromise of SolarWinds' Orion software, used by many government agencies and large enterprises. Attackers inserted a backdoor, SUNBURST, into the software update, allowing them to gain access to numerous organizations, including the U.S. Department of Homeland Security and Microsoft.

REvil (Sodinokibi), active since 2019, became known for high-profile attacks and large ransom demands. Its targets included major corporations such as JBS Foods and Kaseya, affecting thousands of downstream customers. REvil operated as a Ransomware-as-a-Service (RaaS), with affiliates carrying out attacks and sharing profits with the REvil developers.

Finally, Conti ransomware, also active since 2019, is known for its rapid encryption and extensive use of double extortion tactics. Conti targeted various sectors, including healthcare, retail, and manufacturing, and was linked to significant attacks on healthcare institutions during the COVID-19 pandemic, exacerbating the challenges faced by healthcare providers.

These attacks highlight the evolving nature of cyber threats and the importance of robust cybersecurity measures to protect against sophisticated malware and ransomware campaigns.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

## VI. HAZARDS AND IMPACTS

**Data Loss**

Computer viruses can corrupt or delete files, leading to the loss of important data. This can have severe consequences for individuals and organizations, especially if the data is not backed up. Data loss can result in financial losses, productivity disruptions, and the loss of valuable information.

**Financial Loss**

Viruses can cause financial losses in several ways. First, there are the costs associated with repairing infected systems, including purchasing antivirus software, hiring IT professionals, and restoring data from backups. Second, viruses can lead to lost productivity as employees are unable to work due to infected systems. Finally, in the case of ransomware attacks, victims may be forced to pay a ransom to regain access to their files, resulting in financial losses.

**Identity Theft**

Some viruses are designed to steal personal information, such as passwords, credit card numbers, and social security numbers. This information can be used for identity theft and financial fraud, leading to further financial losses and damage to an individual's credit score.

**System Disruption**

Viruses can disrupt the normal operation of computer systems, leading to system crashes, slow performance, and downtime. This can impact productivity and business operations, especially in organizations that rely heavily on computer systems for their day-to-day operations.

**Network Damage**

Worms and other network-based viruses can spread rapidly across networks, causing widespread damage to interconnected systems. This can result in the loss of data, the disruption of network services, and the compromise of sensitive information.

**Reputation Damage**

A virus attack can damage an individual's or organization's reputation, especially if sensitive information is leaked or if the attack results in service disruptions for customers. This can lead to a loss of trust among customers, partners, and stakeholders, which can have long-term consequences for the affected entity.

**Legal Consequences**

Viruses can have legal consequences, especially if they result in the theft or loss of sensitive information. Organizations that fail to protect their systems adequately may be liable for damages and fines under data protection laws. Individuals responsible for creating or spreading viruses may also face legal consequences.

**National Security Threats**

Advanced persistent threats (APTs) and other sophisticated malware can pose significant national security threats by targeting critical infrastructure, government systems, and military networks. These attacks can have far-reaching consequences, including the loss of sensitive information, disruption of essential services, and damage to national security.

**Psychological Impact**

Virus attacks can have a psychological impact on individuals, causing stress, anxiety, and a loss of trust in digital systems and services. This can lead to a reluctance to use computers and the internet, which can impact an individual's ability to work, communicate, and access information.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

## VII. FUTURE TRENDS AND CHALLENGES

As technology continues to evolve, the landscape of computer viruses and cyber threats is also changing rapidly. Here are some future trends and challenges that are expected to shape the battle against computer viruses in the coming years:

**Increasing Sophistication of Malware**

Future computer viruses are likely to become more sophisticated, employing advanced techniques to evade detection and enhance their impact. These may include polymorphic and metamorphic capabilities, which allow viruses to constantly change their code to avoid signature-based detection by antivirus software.

**Rise of AI and Machine Learning in Malware**

Cybercriminals are beginning to leverage artificial intelligence (AI) and machine learning (ML) to create smarter, more adaptive malware. These AI-powered viruses can analyze their environment and make decisions to maximize their spread and effectiveness. They might also use AI to find and exploit new vulnerabilities faster than human hackers can.

**Targeted Attacks on Critical Infrastructure**

There is a growing concern that future malware will increasingly target critical infrastructure, such as power grids, water supplies, and healthcare systems. These attacks can have severe consequences, including loss of life, economic disruption, and national security threats. The increasing interconnectedness of critical infrastructure systems makes them more vulnerable to sophisticated cyberattacks.

**Increased Use of Ransomware and Double Extortion Tactics**

Ransomware attacks are expected to become more prevalent and damaging, with attackers demanding higher ransoms. The trend of double extortion, where attackers not only encrypt data but also threaten to release sensitive information, will likely continue. This tactic increases the pressure on victims to pay the ransom to avoid data breaches.

**Exploitation of IoT Devices**

As the Internet of Things (IoT) grows, so does the attack surface for cybercriminals. Many IoT devices have weak security measures, making them attractive targets for malware. Future viruses may exploit these devices to create large botnets, conduct distributed denial-of-service (DDoS) attacks, or infiltrate networks.

**Evolution of Social Engineering Tactics**

Cybercriminals will continue to refine social engineering tactics to trick users into downloading malware or disclosing sensitive information. Future social engineering attacks may leverage deepfake technology to create convincing audio and video messages, making it harder for users to identify scams.

**Challenges in Detection and Response**

As malware becomes more sophisticated, detecting and responding to threats will become increasingly challenging. Traditional signature-based antivirus solutions may become less effective, necessitating the adoption of advanced behavioral analysis and anomaly detection techniques. Security teams will need to stay ahead of emerging threats through continuous monitoring and threat intelligence.

**Global Collaboration and Legal Challenges**

Combatting the rising tide of sophisticated malware will require increased global collaboration among governments, law enforcement agencies, and private organizations. However, differences in legal frameworks and jurisdictional challenges can complicate these efforts. Establishing international standards and cooperation mechanisms will be crucial in addressing these challenges.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 3, June 2024

**Human Factor and Cyber Hygiene**

Despite advancements in technology, the human factor remains a significant challenge in cybersecurity. Ensuring that individuals and organizations practice good cyber hygiene, such as regular software updates, strong password policies, and awareness training, is essential in preventing malware infections.

**Privacy and Ethical Considerations**

As cybersecurity measures become more invasive to counter sophisticated threats, balancing security and privacy will be a critical challenge. Ensuring that protective measures do not infringe on individual rights and freedoms will require careful consideration and ethical guidelines.

## VIII. CONCLUSION

In conclusion, computer viruses represent a significant and evolving threat to individuals, organizations, and society as a whole. They can cause data loss, financial losses, identity theft, system disruptions, and network damage. Furthermore, viruses can damage reputations, lead to legal consequences, pose national security threats, and have a psychological impact on individuals.

To mitigate these risks, it is essential for individuals and organizations to take proactive measures to protect against viruses. This includes maintaining up-to-date antivirus software, implementing strong cybersecurity practices, and educating users about safe computing habits. Additionally, collaboration and information sharing among cybersecurity professionals, law enforcement agencies, and governments are crucial in combating the growing threat of computer viruses.

As technology continues to advance, the landscape of computer viruses will likely become more complex and challenging. Therefore, it is essential to remain vigilant, adapt to new threats, and invest in robust cybersecurity measures to protect against the ever-evolving world of computer viruses.

## REFERENCES

**[1].** D. V. Pham, M. N. Halgamuge, A. Syed P. Mendis, Optimizing windows security features to block malware andhack tools on USB storage devices, Progress in electromagnetics research symposium, pp. 350-355, 2010.
**[2].** P. Szor, “The art of computer virus research and defense” ,Pearson Education, 2005.
**[3].** Dr. Solomon's Virus Encyclopedia, 1995, ISBN 1897661002
**[4].** Dr. Klaus Brunnstein 1999, from Antivirus to Antimalware Softwareand Beyond http://csrc.nist.gov/nissc/1999/proceeding/papers /p12.pdf
**[5].** Paul Royal, Mitch Halpin, David Dagon, Robert Edmonds, and Wenke Lee. PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware. In The 22th Annual Computer Security Applications Conference (ACSAC 2006), Miami Beach, FL, December 2006.
**[6].** Rainer Link, Prof. Hannelore Frank, August, 2003, Server-based Virus-protection On Unix/Linux
**[7].** Paul Oldfield (2004), Viruses and spam what you need to know. Sophos Plc
**[8].** Wienbar, Sharon (2005), The Spyware Inferno. America Online & The National Cyber Security Alliance.
**[9].** Waqar Ahmad (2003) Computer Viruses as a Threat to Home Users International Journal of Electrical & Computer Sciences King Abdul Aziz University Jeddah. Saudi Arabia.
**[10].** Panda Security (2012),Microsoft Security Intelligence Report, Consumer Reports. Published Available online on http://www.statisticbrain.com/computer-virus-statistics