WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

Technological View of Computer Viruses & Evolution

[1]Pranesh M, [2]Dr V.S. Anita Sofia

[1] Student, [2] Associate Professor
Department of Computer Applications (PG), PSGCAS, Coimbatore.

ABSTRACT:

This study helps us to track down the historical and technological evolution of the computer viruses. This also helps us to understand the way the viruses work and how they affect the function of the computer system. It also deals with the history, classification, and technological evolution of the viruses. In this we also discuses how this viruses can be prevented and development of antivirus solutions.

Keywords: [Viruses, Evolution, History, Technological, Development]

1. Introduction:

The widespread effect of technology has drastically changed how civilizations operate, communicate, and conduct business in the modern digital era. Since the computers were invented , the digital world began and undergone various transitions which has various opportunities and challenges. The most common and long-term problem faced by the digital world is computer viruses which are enduring and constantly changing from the period the computer is invented. Viruses are defined as self-replicating programs intended to used as back door for the attackers and to affect the performance of the system.

The accuracy of digital infrastructure and information systems. This study helps us to characterize the development of the viruses and their historical turning points in the digital world. This study will delve into the historical milestones that define the evolution of computer viruses, from the first known instances in the 1980s to contemporary threats like ransomware and spyware. It will also examine the technological advancements that have both facilitated and countered the proliferation of these viruses. By understanding this dynamic interplay, we can gain insights into current cybersecurity strategies and anticipate future trends in digital threats.

Ultimately, this research highlights the necessity of a comprehensive understanding of computer viruses—not only as technological artifacts but also as reflections of societal concerns and behaviors. As we navigate an increasingly digital world, recognizing the historical context of these threats will be crucial in developing effective defenses and fostering a safer online environment.

1.1 Computer Viruses:

In the modern digital age, the computers plays a crucial role in the everyone's day to day life in every field they became as indispensable part for storing their data's of their work. The major problem they face is the threat of the computer virus. The computer virus is a program which can harm our system and affect the performance of the system, if the virus is not noticed then the virus spread massively and ultimately results in the crashing of the system. Through the various we are able to analyse that the system is affected with the virus. By the variation in the speed of the system, appearance of the pop-up windows, unauthorized log-in and log-out of the systems, etc through this issues one can able to understand that the system is affected with the viruses.

The computer viruses are divided into various types based on the way they affect the computer. Boot virus this affects the boot sectors of the hard disk or floppy disks, Resident virus it is stored in the memory of the system then it affects the other files and programs present in the system, File infector virus by its name it shows first it affects the single file and then it affects the other executable and programs, Space filler virus this virus fills the empty space in the file with virus it cannot be easily detected.

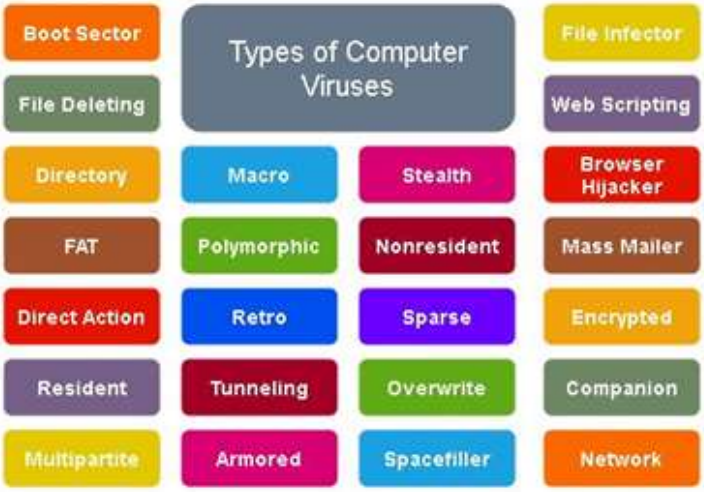

Figure 1. computet virus

2. Literature Review:

The Computer viruses are the threat to the computers in the digital era. They are evolved in various stages according to the technical advancement. This also include about the prevention methods against the viruses.

In the journal "A History of Computer Viruses."(Haffner, D.(2007)) it discusses about the history of the computer viruses and how they are evolved.

The journal "The Spread of Computer Viruses" it deals with spread of the computer viruses and their prevention measures against the virus attacks in the system.

3. Aim and Objective:

This journal's goal is to offer an in-depth knowledge about the computer viruses in the digital era about their origin how they are evolved in the modern age and it prevention methods.

The objective is to investigate the history and evolution of the computer viruses and how they are differentiated.

4. Research methodology:

Take a comprehensive look at all relevant literature, and academic articles related to computer viruses. This will serve as a starting point, help bridge existing knowledge gaps, and set the tone for future research.

4.1 Overview of Viruses:

The virus is a malicious program in which it attack the function and data of the system. In this research we discuss about how the viruses are originated and how the affect the system performance and the functions of the system also learn how to prevent them from the virus attacks and its preventions methods.

4.2 Data Collection:

To do a complete review on the computer viruses, extensive data collection is required. This entails gaining access to a range of resources, such as official government records, cybersecurity reports, scholarly works, policy papers, and professional judgements. Laws and regulations pertaining to cybersecurity, national cybersecurity policies like various laws and organizational structures are present to prevent and create an awareness about the virus attacks and the preventive measures against the virus attacks.

4.3 Types of Computer Virus:

The computer viruses are the malicious program that affects the computers. These viruses are differentiated into various types based on their behavior, propagation method, and the impact they create in the system. The different virus are File infectors, Macro virus, Boot sector virus, Resident virus,

Worms, Network virus, etc. these are the classifications of the viruses, and due to their evolving nature the threats caused by these viruses are also increasing, so the cybersecurity measures also need to be taken accordingly.

5. Notable Computer viruses:

In this paper we will study about the viruses that have a certain impact in the computer through this viruses the scope of the cybersecurity and the public awareness of digital threats are increased. This viruses are difficult to control when the outbreak happened, these virus are hard to control because of its propagation method and impact.

Creeper Virus:

This virus occurred in the year of 1971. Many individuals consider that the Creeper virus was the first computer virus. It was created by Bob Thomas as an experimental program with the goal of wandering between computers linked to the ARPANET and displaying the message, "I'm the creeper, catch me if you can!" Although it did no harm, it led initial concerns about computer security and set the stage for later self-replicating programs.

ILOVEYOU virus:

This virus led its outbreak in the year of 2000. ILOVEYOU, was among the most infamous viruses, propagated by email in what appeared to be a sentimental note. Opening it caused malware to overwrite files and send copies of itself to all of the user's email contacts. The malware exposed human behavior's susceptibility in cybersecurity, resulting in an estimated $10 billion in losses globally and increased awareness of social engineering techniques.

The Code Red Worm:

This virus led its outbreak in the year of 2001. This virus targets the vulnerability in the software and the windows servers running IIS. It infected over 359,000 machines in a matter of days, causing a great deal of disruption and downtime. The worm gained notoriety for its quick spread and straightforward yet potent assault strategy, underscoring the importance of applying updates and patches for software on time.

The Blaster Worm:

This virus leads a outbreak in the year of 2003. By taking advantage of a flaw in Windows, the Blaster worm made affected machines crash and reboot their systems. Additionally, it made an effort to assault Microsoft's website with a distributed denial-of-service (DDoS) attack. Blaster's extensive effects sparked conversations on patch management's significance and the demand for more robust network defenses.

The Storm Worm:

This virus leads to an outbreak in the year of 2007. Often propagated through spam emails with attention-grabbing subject lines, the Storm Worm was renowned for its polymorphism and its use of social engineering. It built a vast botnet that was used to launch DDoS attacks and spread other malware. The Storm Worm brought to light the difficulties in countering coordinated cybercriminal activities and the malware's increasing sophistication.

This above mentioned viruses are the notable viruses that shaped the idea towards the virus and the main importance of the cybersecurity. In outbreak of the each viruses it helped the digital world to emphasize the importance of the prevention method against the viruses.

6. Evolution of virus detection and prevention:

In the recent days the virus detection and the preventions are helpful for the cybersecurity professionals to prevent the attack of the virus. Both the detection and prevention techniques for computer viruses have advanced with time. In addition to emphasizing significant advancements and difficulties faced by cybersecurity professionals, this section provides a historical evolution of virus detection and prevention tactics.

Early Detection Method:

Originally, antivirus software used straightforward signature-based techniques to detect viruses by identifying known virus signatures, which are particular code strings. Although early antivirus software, like McAfee and Norton, successfully applied this strategy, they had difficulty combating novel and unfamiliar malware. With the emergence of polymorphic and metamorphic viruses, which can change their coding to avoid detection, the shortcomings of signature-based detection became clear.

Behaviour-Based Detection:

Technology progressed and resulted in behavior-based detection techniques that watch apps in real time to spot fraudulent activity. By being proactive, malware can be found while it's being executed instead of after it has already infected the system. The importance of behavior-based detection has grown as sophisticated malware, including ransomware, has begun to exploit zero-day vulnerabilities.

Nowadays due to the advancement in the technologies there are various other virus detection methods are implemented, like Cloud-based, Machine Learning and AI.

Cloud-based Detection:

Cloud-based antiviral solutions became popular in the 2000s as cloud computing gained popularity. Detecting and analyzing malware on several devices, these systems offer real-time updates and improved detection capabilities by utilizing the strength of centralized databases. Through the analysis of millions of user data, cloud-based systems can detect new risks faster, facilitating the sharing of threat intelligence.

Through the help of these detection methods we are able to prevent the attack of the virus and prevent the system from another virus attack.

7. Legal and Ethical Implications:

Legislation, company practices, and society norms have all been impacted by the proliferation of computer viruses and malware, which has also created serious legal and ethical considerations. These ramifications are examined in this part, along with the difficulties and obligations that people, businesses, and governments must deal with in the digital era.

Numerous nations have passed legislation to combat crimes involving computers, such as the unapproved development and dissemination of viruses. Crucial legal structures include, The United States has the Computer Fraud and Abuse Act (CFAA), which makes it illegal to distribute malware and gain unauthorized access to computer systems.

The objective of the Council of Europe's Convention on Cybercrime, often known as the Budapest Convention, is to promote international cooperation in the fight against cybercrime by standardizing laws across its member states.

Intellectual property rights are frequently in conflict with the production and dissemination of viruses. Malware that violates copyright or improperly utilizes proprietary code, for instance, presents difficult legal issues. When creating security software, businesses have to deal with intellectual property concerns to make sure they safeguard their own assets without unintentionally infringing on the rights of others.

Developing secure systems is a major ethical duty for software engineers. When vulnerabilities are found, disclosure becomes ethically problematic. In order to reduce the possibility of exploitation, responsible disclosure entails contacting those who may be impacted and giving them time to fix any vulnerabilities before making the issue public.

In order to find weaknesses and safeguard systems, ethical hackers, sometimes known as "white hats," are essential. Still, their research presents moral dilemmas about privacy, permission, and the possibility of abusing vulnerabilities that are found. To ensure that their acts benefit cybersecurity without violating people's rights, it is imperative that clear principles and ethical standards be followed.

The public is now more aware of cybersecurity concerns as a result of high-profile viral outbreaks like WannaCry. Better corporate security procedures and a rise in demand for cybersecurity education are two benefits of this heightened awareness. However, it also brings up moral concerns about inciting fear and portraying technology as essentially harmful.

8. Future trends in viruses and prevention:

Computer viruses and cybersecurity are dynamic fields that are always changing as technology develops. The future of cyber threats and countermeasures is examined in this section along with some developing trends and predictions.

With cutting-edge methods like artificial intelligence and machine learning, the next wave of malware is probably going to be considerably more complex. Using artificial intelligence (AI), cybercriminals can develop highly adaptive malware that can learn from its surroundings and become more difficult to identify and remove. Conventional detection techniques will be put to the test by this evolution, requiring novel cybersecurity strategies.

With the proliferation of IoT devices, vulnerabilities in these connected systems pose significant risks. Many IoT devices lack robust security measures, making them attractive targets for cybercriminals. Future cybersecurity efforts will need to address the challenges of securing a vast and diverse array of devices, ensuring that proper protocols and standards are in place to protect user data and privacy.

Collaboration amongst stakeholders—governments, businesses, and cybersecurity experts—will be essential as cyber threats continue to escalate in complexity. Initiatives for information exchange will assist firms in staying up to date on new threats and efficient defenses. Public-private collaborations can strengthen cybersecurity resilience overall and facilitate better incident response.

9. Conclusion:

Technology improvements, cybersecurity precautions, and the wider societal ramifications of digital dangers interact intricately, as demonstrated by the study of computer viruses and their evolution. The world has changed significantly over the years, posing constant difficulties for people, businesses, and governments. Aside from demonstrating the dynamic nature of these dangers, the historical background of well-known computer viruses also teaches valuable lessons about creating detection and preventive tactics. Heuristic analysis, behavior-based detection, and AI-driven solutions are examples of increasingly sophisticated techniques that have replaced the earlier reliance on signature-based detection, as we have seen. These developments highlight the necessity of modifying security procedures to fend against threats that are getting more complex.

When it comes to legal and ethical issues, the cybersecurity plays a very important role in the prevention of the virus attacks, there are also various organizations which are helpful in the prevention of the virus attacks.

References:

[1] *"Computer viruses: Theory and experiments." Computers & Security, 5(4), 343-346, Cohen, F. (1986).*

[2] *"History of computer viruses." , Symantec. (2020).*

[3] *"On the Risks of Software." ACM SIGSOFT Software Engineering Notes, Cohen, F. (1983).*

[4] *"A History of Computer Viruses." Computer Security Journal, Haffner, D. (2007).*

[5] *"Crypto-Lockers: A Comparative Study." International Journal of Information Security, Kharraz, A., et al. (2015).*

[6] *"Machine Learning for Cybersecurity: A Review." IEEE Transactions on Information Forensics and Security, Srinivasan, S., et al. (2021).*

[7] *"IoT Security Threats." Internet Security Threat Report, Symantec. (2019).*

[8] *"The Spread of Computer Viruses." Journal of Computer Science, Turing, A. (2000).*