VIRUS

Assignment-01

Group - 01

IS2107
Social & Professional Issues

09/05/2024

Table of Contents

1. Introduction

Malicious software applications created to replicate and spread throughout computers and networks are known as computer viruses. They have the ability to do significant harm to specific users, companies and society at large. They often behave as legitimate applications or files. Viruses can infect computers through a variety of methods as examples,

- email attachments.
- internet downloads.
- contaminated portable media.

It is extremely risky for the computer.

“There are three components to a comprehensive technical policy against computer viruses: preventing them from infecting your sonware, detecting and containing them once they have entered your system, and recovering from an infection once viruses have been detected.”[1]

2. Process

Computer viruses usually infect data or the boot area of a hard drive. Once stimulated they have the ability to undertake a number of damaging acts, including data corruption, personal information theft, and system function disabling. Computer Virus link to an executable host file. Therefore, When the file is decrypted, their virus code is executed. The viruses can quickly propagate through networks, infecting multiple computers within a company or across the internet.[2]

3. Impact on Computer Users and Society

The impact of computer viruses can be severe on both individual users and society at large . For individual users virus can result in,

- Data loss
- Identity theft
- Financial loss
- System crashes

spreading viruses can affect sensitive information and public trust in online platforms.

“The term „computer virus“ was formally defined by Fred Cohen in 1983, while he performed academic experiments on a Digital Equipment Corporation VAX systems”

4. Specific Safety Measures

To relieve the chance of infection diseases, computer clients and organizations ought to execute the taking after security measures.

- Introduce a trustworthy antivirus program and keep it overhauled routinely to identify and expel infections.
- Be careful when opening email connections or clicking on joins from obscure or suspicious sources.
- Keep working frameworks, computer program applications, and security patches up to date to address known vulnerabilities.
- Use strong, unique passwords for online accounts and enable two-factor authentication whenever possible.
- Routinely reinforcement imperative information to an outside capacity gadget or cloud benefit to play down the effect of an infection disease.

“Viruses have developed from simple locally operating file infectors to quickly spreading Internet worms capable of executing in stealth, without user intervention and without touching any files on the system.”[3]

5. Examples

Several examples of computer viruses have caused widespread damage over the years,

- **Melissa Virus**

  Spread through e-mail in 1999, causing mail servers to end up over-burden and disturbing email administrations around the world.

- **Conficker Worm**

  To begin with, identified in 2008, this worm abused vulnerabilities in Windows working frameworks to contaminate millions of computers and make an enormous botnet.

- **WannaCry Ransomware**

  In 2017, WannaCry ransomware infected hundreds of thousands of computers in over 150 countries, encrypting data and demanding ransom payments for decryption keys.

6. Additional Details

- Some viruses has being designed to exploit specific vulnerabilities in software or hardware It making them particularly difficult to detect and remove.
- The proliferation of internet connected devices has expanded the potential attack surface for viruses including smartphones, tablets, etc.
- Some Law enforcement agencies and Cybersecurity experts continually monitor and investigate virus related threats to prevent and minimize their impact on computer users and the society.

7. References

[1] Spafford, E. H., Heaphy, K. A., & Ferbrache, D. J. (1989). A computer virus primer.

[2] Dwan, B.(2000) “The Computer Virus — From There to Here.: An Historical Perspective” Computer Fraud & Security, 2000(12),pp. 13-16

[3] Reinikainen, M. (2019). Computer viruses (Master's thesis, Itä-Suomen yliopisto).

8. Group Members

21CIS0017 - Mayura

21CIS0114 - Maduranga

21CIS0060 - Hasini

21CIS0062 - Rashmi

21CIS0118 - Kavini

21CIS0122 - Navini

21CIS0213 - Kushan

21CIS0238 - Harishihan