Review on Computer Virus and Malwares

Dr.S.Narayanan[1], Dr.C.Sabarigirinathan[2], Dr.K.Vinayagavel[3], Dr.D.Deepiha[4]

[1](PhD student)

[2](Professor and HOD, Dept of Prosthodontics, Tamilnadu Govt Dental College & Hospital, Chennai, India)

[3](Professor, Dept of Prosthodontics, Tamilnadu Govt Dental College & Hospital, Chennai, India)

[4](Post Graduate Student, Dept of Prosthodontics, Tamilnadu Govt Dental College & Hospital, Chennai, India)

Abstract :

Computer virus is a programme that is not oriented towards the computer user and its actions do not serve the interests of computer user. The virus is meant to disrupt the work of the computer. In order to secure your files and for sensible use of your working time you should use antivirus software in your computer. In this article, you will find explanations regarding computer viruses and antivirus software.

Introduction :

A virus is a computer code or program, which is capable of affecting your computer data badly by corrupting or destroying them.

Computer virus has the tendency to make its duplicate copies at a swift pace, and also spread it across every folder and damage the data of your computer system.

A computer virus is actually a malicious software program or "malware" that, when infecting your system, replicates itself by modifying other computer programs and inserting its own code.

Infected computer programs may include data files, or even the "boot" sector of the hard drive.

Types of Virus

Following are the major types of computer virus −

Worms

This is a computer program that replicates itself at a swift pace. Unlike a computer virus, it is self-contained and hence does not need to be part of another program to propagate itself.

Trojan Horse

A Trojan Horse is also a sort of destructive program that remains disguised in a normal software program. It is not exactly a virus, as it cannot replicate itself. However, there is possibility that virus program may remain concealed in the Trojan Horse.

Bombs

It is similar to Trojan Horse, but Logic bombs have some specialty; these include a timing device and hence it will go off only at a particular date and time.

How Does Virus Affect?

Let us discuss in what ways a virus can affect your computer system. The ways are mentioned below −

- By downloading files from the Internet.
- During the removable of media or drives.
- Through pen drive.
- Through e-mail attachments.
- Through unpatched software & services.
- Through unprotected or poor administrator passwords.

Impact of Virus

Let us now see the impact of virus on your computer system −

- Disrupts the normal functionality of respective computer system.
- Disrupts system network use.
- Modifies configuration setting of the system.
- Destructs data.
- Disrupts computer network resources.
- Destructs of confidential data.

Virus Detection

The most fundamental method of detection of virus is to check the functionality of your computer system; a virus affected computer does not take command properly.

However, if there is antivirus software in your computer system, then it can easily check programs and files on a system for virus signatures.

Virus Preventive Measures

Let us now see the different virus preventive measures. A computer system can be protected from virus through the following −

- Installation of an effective antivirus software.
- Patching up the operating system.
- Patching up the client software.
- Putting highly secured Passwords.
- Use of Firewalls.

Most Effective Antivirus

Following are the most popular and effective antivirus from which you can choose one for your personal computer −

- McAfee Antivirus Plus
- Symantec Norton Antivirus
- Avast Pro Antivirus
- Bitdefender Antivirus Plus
- Kaspersky Anti-Virus
- Avira Antivirus
- Webroot Secure Anywhere Antivirus
- Emsisoft Anti-Malware
- Quick Heal Antivirus
- ESET NOD32 Antivirus

Computer Related Securities :

Cybersecurity refers to preventative methods used to protect information from being stolen, compromised or attacked.

Passwords are a cybersecurity tool that people encounter nearly every day. Other common cybersecurity tools include:

- Anti-virus/anti-malware software
- Software patches
- Firewalls
- Two-factor authentication
- Encryption

Data security refers to protective digital privacy measures that are applied to prevent unauthorized access to computers, databases and websites. Data security also protects data from corruption.

Examples of data security technologies include backups, data masking and data erasure.

One of the most commonly encountered methods of practicing data security is the use of authentication. With authentication, users must provide a password, code, biometric data, or some other form of data to verify identity before access to a system or data is granted.

Internet security is a catch-all term for a very broad issue covering security for transactions made over the Internet. Generally, Internet security encompasses browser security, the security of data entered through a Web form, and overall authentication and protection of data sent via Internet Protocol.

Internet security is generally becoming a top priority for both businesses and governments. Good Internet security protects financial details and much more of what is handled by a business or agency’s servers and network hardware. Insufficient Internet security can threaten to collapse an e-commerce business or any other operation where data gets routed over the Web.

Anti virus and Encryption :

Anti-virus software is a software utility that detects, prevents, and removes viruses, worms, and other malware from a computer. Most anti-virus programs include an auto-update feature that permits the program to download profiles of new viruses, enabling the system to check for new threats. Antivirus programs are essential utilities for any computer but the choice of which one is very important.

Clockwise
a. Avast
b. Avira
c. Kaspersky
d. McAfree
e. 360 Total Security

Popular Antivirus Software Logos

Encryption is the process of using an algorithm to transform information to make it unreadable for unauthorized users. This cryptographic method

protects sensitive data such as credit card numbers by encoding and transforming information into unreadable cipher text.
This encoded data may only be decrypted or made readable with a key.
Encryption is essential for ensured and trusted delivery of sensitive information.

Encryption Icon

TYPES :
Symmetric-key encryption uses two secret, often identical keys or codes for computers involved in message transmission. Each secret key's data packet is self-encrypted. The first symmetric encryption algorithm is the Data Encryption Standard (DES), which uses a 56-bit key and is not considered attack-proof. The Advanced Encryption Standard (AES) is considered more reliable because it uses a 128-bit, a 192-bit or a 256-bit key.

Asymmetric-key encryption also known as public-key encryption, uses private and public keys in tandem. The public key is shared with computers attempting to communicate securely with the user's computer. This key handles encryption, rendering the message indecipherable in transit. The private matching key remains private on the user's computer. It decrypts the message and makes it readable. Pretty good privacy (PGP) is a commonly used public-key encryption system.

Conclusion :
Like a human virus, a computer virus can be dangerous and possibly infectious to other computers. They can be spread between computers, and can also be transported via email, USB drives and other types of media.
Hence not having antivirus on a computer is like inviting a criminal into the house or having an uninvited guest. Antivirus software is the "policeman" at the gate of the computer system. And so the importance of Antivirus Software should not be underestimated.

Reference:

1. Computer Awareness program Version 1.0, NIIT

2. Absolute Beginner's Guide to Computer Basics, Second Edition, By Michael Miller
3. Basics of Computer Science, Rajiv Khanna
4. Computer security Basics, Rick Lehtinen, G.T. Gangemi Sr.
5. Computer and Network Basics, Lisa Donald