ITMR

योगः कर्मसु कौशलम्

WHITE PAPER ON

Antivirus

Prepared by **Mohammed Samiuddin**

Contents

Introduction

A “Computer virus” is a software program or code that replicates itself and spreads from one computer to another without the users’ permission. An entry of this code in any computer drastically interferes with the operation and function of the computer. Such codes are usually attached to programs like Excel, Word, Outlook and PowerPoint. When these programs are run, the virus attached to it is triggered to run, which causes wide range of problems including file corruption, data deletion, and email spamming. Since then individuals and organisations began to develop strategies for antivirus software.

‘Antivirus’, is a term given to protective software that are specifically designed to protect computers from all kind of viruses harmful to a computer system. It also gives protection against malicious software that include viruses, key loggers, hijackers and Trojan. Antivirus perform tasks such as preventing virus, scanning and detecting virus, removing virus from infected files and recovering the infected files.

Before internet connectivity was widespread, viruses were typically spread by infected floppy disks. However, as internet usage became common, viruses began to spread online.

Computer viruses are highly prevalent in the present day world. A new virus is introduced every day, so the computers must be updated at regular intervals to ensure it is free from viral infection.

Today, most antivirus products use a combination of reactive and proactive technologies. Hence, the basic function of an antivirus software is to provide complete protection against malicious software and other virus definitions. Since, there are many virus writings created each day, many of the antivirus authors are including several other functions within the program. If the computer is not protected with security software, it gets highly prone to infective malware that will not only infect the machine, but will also expose all the personal data of the user that can be used by criminals for unlawful acts. A good security software will be a combination of firewall, antivirus software, and anti-spyware.

What is the need for Antivirus?

The need of antivirus is:

- To detect the presence of threat, if any
- Real-time protection against malwares and viruses
- To make the applications and data secure in a particular system
- To increase the performance of system

Symptoms of Virus Attack

Virus attacks in the computer can be identified by:

System Performance

- Appearance of different pop-ups and messages
- Computer runs slower than usual
- Computer no longer boots up
- Display screen flickers
- PC speaker beeps periodically
- System crashes for no reason
- Files/directories sometimes disappear
- Denial of Service (DoS)

The Internet

- Issues in connecting to the Internet
- The Internet Explorer page may not be displayed
- Default home page will be changed
- Redirected to different pages than the intended
- Unexpected/unwanted toolbars are added to the browser
- Numerous web messages and pop ups
- The web browser hangs

The Mailbox

- Mails will be displayed without subject and sender email address
- Bulk spam mails are sent from the mailbox

Virus Detection Techniques

Typical antivirus software uses different techniques for the purpose of securing the operating system / computer system.

Signature based Detection / Virus Dictionary Approach

- The antivirus application refers to a dictionary of virus signatures that have been known by the developer of the application
- In case, any code within a file matches with the virus dictionary, the antivirus software performs to either delete that code or quarantines
- Files are examined when they are created, opened, closed or e-mailed by the antivirus application. Requires regular updates in order to prevent the virus dictionary from getting outdated

Heuristics-based Detection

- This method aims at identifying malwares by checking files for suspicious characters without exact signature match
- When several suspicious characters are detected in a file, it is flagged as malicious

Behavioural Detection / Suspicious Behaviour Approach

- This is a contrast antivirus application approach where the functionality is to monitor the behaviour of the programmes
- If an application is behaving to access the data of another application or to manipulate its functionality, such an action is considered as suspicious and the user is directed by the software for a quick and an effective action

This approach provides protection against all viruses including the ones that are not available in the dictionary.

Sandbox Detection Approach

- Using a sandbox detection method, the antivirus application emulates the beginning code of every brand new program execution

After the program is closed, the sandbox is analysed for changes made within it and the presence of virus is indicated.

Cloud-based Detection

- In this approach, the antivirus software searches for malware in the protected computers on the provider's infrastructure. This is done by capturing the file details and processing it in the cloud engine
- The cloud engine derives the behaviour of malware by comparing the data from various systems

How to choose the best fit Antivirus?

Computer users have unlimited choices for selecting antivirus application. There are trial offers as well as commercial versions that can be easily obtained from the web. Despite of the quantity, it is still a daunting task to select an antivirus that will work best with the system. Every antivirus solution should offer Performance, Protection, Regular updates and Transparency. These are fundamental requirements and should not be compromised.

Performance

The solution must not impact the computer's performance in any way. Performance degradation adds significantly to the total cost of any solution, and many users unknowingly tolerate this degradation.

Protection

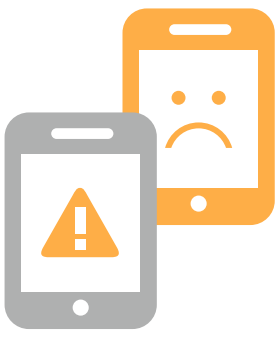
The solution must not allow a system to get infected. The main reason behind having an antivirus installed (investing in keeping it updated) is to be protected, not infected.

Regular Updates

If the antivirus software is termed as effective, it should regularly check for the latest updates without any manual intervention. With viruses multiplying enormously, the antivirus software requires updates every day. An effective antivirus software will run at the background and get updated.

Transparency

If the solution is difficult to use or manage, it becomes liable and consumes more effort for maintenance activities. The effort spent on maintenance can be utilised productively for building a competitive edge for the business. If the solution is not transparent (i.e. invisible) to users, they are tempted to turn it off; when that happens the system is prone to security risks.



Cautious / Preventive Techniques

There are numerous ways by which a system can be attacked and private data can be stolen by hackers and other attackers in spite of installing efficient antivirus software. Hence, it is an individual's responsibility to adhere with few guidelines to protect themselves from attacks:

- Install one antivirus software only
- Do not disable the antivirus software
- Download software from trusted sources
- Keep software updated
- Track Warnings and Alerts
- Consider a complete Security Suite
- Scan Additional Devices

Conclusion

Virus is meant to interrupt the computer operations, corrupt the data stored on the hard disk, create access rights for hackers and slow the computer network by creating excess network traffic. To prevent data theft, users must install antivirus software. Although the antivirus software do not offer full guarantee of protection, they help user in detecting and alerting the presence of virus. Different antivirus software are good at tackling different problems. With increase in the types of malwares, the antivirus vendors are incorporating several layers of detection in their tools. Among the available antivirus software, users must select the right option essential for protecting their devices.

About the Author

Mohammed Samiuddin spearheads the branding aspects & managing client relationships of ITMR. His passion includes speaking on cyber security threats, data security practices and new technological areas.

Reference

http://EzineArticles.com/4862743

http://www.slideshare.net/ComputerAdvisor/the-difference-between-anti-virus-and-internet-security

http://www.slideshare.net/singhhp10699/11-virus-vs-antivirus

http://www.projectvrc.com/blog/12-antivirus-impact-and-best-practices-on-vdi

http://en.wikipedia.org/wiki/Antivirus_software

http://www.gficloud.com/uploads/Antivirus_management_in_the_cloud_A4.pdf

http://kb.eset.com/esetkb/index?page=content&id=SOLN2563

Antivirus Myths and Facts: By Helmuth Freericks

http://searchsecurity.techtarget.com/tip/How-antivirus-software-works-Virus-detection-techniques

About ITMR

Institute of Technology, Management and Research (ITMR), a division of Mamta Trust, is a premier institute that provides world class professional training programs for the corporates and academic sector. ITMR's motto 'yogah karmasu kausalam' means 'Yoga is excellence in action' and is the foundation of its vision to evolve into a "CENTRE OF EMINENCE" to offer cutting edge vocational skills and mold professionals to become business and technical domain experts. ITMR's professional and corporate training programs include several cutting edge to help working professionals acquire domain expertise and meet the current and emerging challenges in the IT world.

Our flagship training program on Cyber security has (PDCIL) Professional Diploma in Cyber Investigations and Laws is a top of the class cyber security program in the country that trains top officials in the Police departments, Indian and International Banks, Military, Legal fraternity, Fortune 100 Global companies and Blue Chip India IT companies.

ITMR also offers research programs on Cyber Security (network security monitoring and access products), in association with Secure IQ, a leading provider of network security software products with headquarters in Fairfax, Virginia, USA and operations and development in Chennai, India.

Institute of Technology Management & Research
(Division of Mamta Trust)
2/850, Mugaliwakkam Road, Mugaliwakkam, Chennai - 600 125, Tamil Nadu, INDIA.
Admin Office: HTC Towers, No.41, GST Road, Guindy, Chennai – 600 032,
Tamil Nadu, INDIA. Phone: +91 44 4345 3500 / +91 44 4345 3349
Contact for More Information: training@htcitmr.ac.in