Volume 4, No. 1, January 2013
Journal of Global Research in Computer Science
ISSN-2229-371X
REVIEW ARTICLE
Available Online at www.jgrcs.info

SECURITY ISSUES IN PROTECTING COMPUTERS AND MAINTENANCE

S.Rajeshwari[1], V.Saravanan[2]
[1]UG Scholar, IT Department, P.S.V. College of Engineering and Technology, Krishnagiri, Tamilnadu, India
rajaaeswaris@gmail.com[1]
[2]Asst. Prof. IT Department, P.S.V. College of Engineering and Technology, Krishnagiri, Tamilnadu, India
v_saravanan18@yahoo.co.in[2]

Abstract: Today maintaining computer system is a big challenging task, since the virus programs easily spreads to the computer via pen drive, floppy disk, optical disks, Local network and Internet connections…etc. Other reasons like frequent power failure, unexpected mistakes done by users like deleting, editing and configuring of system files and system instability due to errors in various hardware will corrupt the files and the data loss may occur. In this paper we have given solutions and suggestions for maintaining computer systems without using antivirus software. Our suggested solution minimizes the impact of the above said factors and makes the computer systems work reliable.

Keywords: Virus, Backup, Restore, System Maintenance.

INTRODUCTION

Nowadays everyone uses computers for personal works and official works. We can classify the users in to three major groups based on their usage; home users, mobile users and online users. Generally the home user uses the computer for multimedia purpose. They will not use the Internet frequently. The chances of system crash may due to frequent power failures, voltage fluctuations and some virus spread through storage devices like pen drive. Generally the mobile users uses the laptop like devices for storing some personal data and they will connect the Internet more frequent than the home users for some purpose like mail check etc.. The mobile devices will have the battery backup and the system crash may not occur due to power failure. Other reason such as virus infection for pen drive like devices and Internet may crash the system. The online users use the computer for accessing Internet and the reason for system crash will be the virus infection from Internet, pen drivel like devices and power failure (high chances due to virus infection).

Myth on antivirus software:

Most of the users think that by installing antivirus software they will get 100% protection from virus. But in reality, no antivirus software can give complete protection from the virus. The reason for this is, each and every day a new type of virus programs are developed by the virus programmers throughout the world. The information about the newly created viruses may not be known to the antivirus software until it gets updated. The information about the virus programs are maintained by the antivirus software as a virus database. This database has to be updated frequently to enable maximum protection (Within that all the folders including antivirus can be infected by viruses). Even after updating the virus database, the information about newly released virus programs may not available. Also, two or more antivirus software developed by different software corporations may not have equal set information about the virus in the virus databases. So, it is clear that no antivirus can able to give complete protection against virus.

Myth on UPS:

Uninterrupted Power Supply (UPS) will regulate the voltage level from fluctuations and it will provide power to the electrical devices even after the power failure. It will charge the battery when the power available and it regenerate the power during the power failure by utilizing the power already stored in the battery. Most of the users think that, by installing UPS they will get maximum protection. But it is not true in real. Everyone knows that each and every battery has a limited power backup and UPS can works for a limited number of time duration if the power failure is too long. Especially in the rural areas the power failure may occur more than an hour frequently in many countries. If something goes in the UPS hardware then the voltage level and/or frequency of the generated power may change. This will make the system unstable. So, even after implementing the UPS the power failures may not be avoided with 100% guaranty. The UPS backup time depends on the current load and charge level of the battery.

Myth on external storage devices:

Today many digital types of equipment like computer systems, CD/DVD players, Audio Systems, Video game players and Latest TVs provide USB interface to make use of the pen drive like storage devices. So the usage of pen drive increased every year than the other storage devices. The virus developers focus more on pen drive like devices to spread the virus programs. When the users insert the pen drive like devices in to the computer system, the virus will get spread automatically from the pen drive to the computer without the knowledge of users. Similarly, if the user inserts a good pen drive (Without virus) into the computer that has infected already by the virus, then the virus programs will get copied to the pen drive like devices automatically without the knowledge of user. User thinks that by installing antivirus software and by scanning the pen drive before opening it may delete the virus programs completely. But in real the antivirus software may not remove the virus code completely from the pen drive like external storage devices.

Hence, to protect the computers from unexpected crashes and data losses we need to find different solutions and methods for system maintenance and recovery process.

VIRUS

Just like other software, virus is also a computer program which can do anything in the computer. Any software may develop in such a way that it shall not perform any harmful task to the system and data. Software will perform one or more tasks to accomplish a specific work. The behavior of the software will remain same forever. Virus is also like software which will perform harmful task to the computer system. Virus programs will spread it automatically using storage devices and network connectivity. Few viruses are harmless, some viruses will delete the system and data files and other viruses will corrupt the system and data files. After the virus infection the operating system will start malfunctioning and the performance of the system will be spoiled.

Most of the virus works as a background process so that the user of the computer may not know about the virus infection in his system until the system starts malfunctioning. It is better know about the spreading of virus to prevent it.

Spreading of virus through storage devices:

Today nobody is using the floppy disk and drive because of its low capacity, speed and reliability. The optical storage devices like CD, DVD and Blue ray disk drive were used by most of the users for backup purpose. Most of the home users use these disks for storing multimedia elements, especially to store video and audio files. The content of these disks will not get changed during time, since most of disk is ROM (Read Only Memory). If the disk content contains virus, then throughout its life time the virus cannot be healed (If it is a rewritable disk then the virus can be destroyed). During the burning process we must ensure that the files are virus free to avoid spreading of virus. In case of pen drive like devices (Including memory cards) the virus will get spread easily. At the same time the virus can be deleted at any time.
The virus can be spread to these storage devices using the following.

a. Already available executable setup files
b. Html files
c. Shortcut files
d. Executable files
e. Autorun.inf file
f. Batch files (.BAT)

Spreading of virus through Setup files:

If a system gets infected by virus then the system will start copying the virus codes inside the executable setup files which is already stored in the hard disk or in the removable devices. If the setup files is shared and installed in other computers, then along with the software installation virus code will also execute in the background. There after the virus code will be copied in all the setup files in that destination system. This is how the virus will spread through the setup files.

Spreading of virus through Html files:

The infected html files may contain virus code in the form of VB script or Java script. These scripts will get executed at the time of opening the infected html files using the browsers. The offline web pages stored in the computer system will be edited by the virus program and the harmful scripts will be added to the offline files. If this offline html files are shared and opened in another system, then these scripts will get executed and the virus will get spread in the destination system.

Spreading of virus through Shortcut files:

Few virus files will get stored in the hidden folders as a hidden file and these files may not visible to the user. For such virus files shortcuts are generated which is visible to the users. If the user open the shortcut files by mistake then the hidden virus files will get execute and the infection will start.

Spreading of virus through executable files:

Few viruses will hide the normal folders and it will create an executable file in the name of hidden folder. The icon of the executable file may look like the folder symbol. On seeing this files user may think that it is their normal folder and they may open it which makes the virus to execute. Some virus will be stored as a normal or hidden executable file with some attractive name and icons. This will attract the user and make the user to open it.

Spreading of virus through Autorun.inf file:

Autorun.inf is a file through which the operating system provides the facility of auto play. Generally, after inserting the storage devices or medium in to the computer, the user has to open it manually for accessing the content. But with the help of autorun.inf file, the manual work can be automated. The autorun.inf file contains the information like which file has to be executed automatically at the time of inserting the medium and what icon the storage medium should have in the computer. The viruses use this autorun.inf facility for executing itself in the destination computer automatically. Because of this infected autorun.inf files, the virus spreads easily in all computers through pen drive like devices without the user knowledge, immediately after the insertion of such devices.

Spreading of virus through Batch files (.BAT):

The batch files are used from the time of DOS operating system, for arranging a group tasks in a specific order. During the system boot process a special batch file "autoexec.bat" will be executed by the operating system. The main usage of this batch file is for setting the default paths and executing essential software which is required for providing a specific service. Virus will use this particular facility to run its code each time the system gets started.

Spreading of virus through network connectivity:

In this section 1.1 we have discussed how the virus will get spread through the storage devices. Now in this section we will discuss how the virus get spreads through network and Internet connectivity. A special type of virus called "worm" will spread through the network without any user interaction. This type of virus utilizes the large amount of network bandwidth (May increase the network usage charge if it is not an unlimited pack) and system memory and makes the network and system responding slower than the normal speed. It makes the attackers to access your system from the remote and it will increase the security risk. Generally the virus will spread using the following ways

a. Downloading of executable files
b. Opening web pages from intranet and Internet

Spreading of virus through file download:

The computer users like to download software and games from the Internet. The software and game will be in the form of executable file. As said in the section 1.1 through executable files virus can spread easily. Many sites in the internet contain infected executable files and by downloading it, the user system may get affected by virus.

Spreading of virus through web pages:

Using browsers the user will open the web page and if that page contains harmful scripts in it then it will damage the system by spreading the virus. Also by allowing plug-ins and activex controls to get installed in our system the security risk will increase further. For online users this type of risk is very common and frequent.

PREVENTING VIRUS INFECTIONS

In this section we have given tips and tricks to prevent virus spreading to the computer system. As said in section 2, some virus will spread automatically and other will spread by user interaction. We can prevent the virus spread by user interaction easily than the automatically spreading virus.

Preventing virus infection from external storage devices:

The "autorun.inf" file makes the virus infected files to execute automatically. Deleting this autorun.inf file is not a easy task in virus infected system. This autorun.inf file will be generated again and again even after deleting it. To stop this copy of autorun.inf file, we can create a folder with the name autorun.inf in the external storage devices. This folder can be deleted by the virus and once again the autorun.inf will be generated. To avoid deletion of this folder we should make the folder undeletable. This can be done in many ways depending upon operating system. By using the utility software like "USB Disk Security" this can be done easily. The software has a facility to disable autorun feature. By using such software, undeletable folder with the name autorun.inf will be created in all external storage devices connected to the computer.

The autorun feature can be disabled by changing the values of windows registry using registry editors. But that is possible for the advanced users and too complicated and not recommended for the normal users. These are the ways how we can stop the automatic virus execution.

After disabling the autorun facility the next work is to delete all the executable virus files. Most of the virus files are very similar to the original folders, differentiating them is very difficult. For differentiating the virus and folders we can use the search option in windows by right clicking the storage device icon and selecting search option from the popup menu. In the search window, searching file name should be as "*.inf, *.exe, *.htm, *.html". Also by using "more advanced options" in the search window, three check boxes namely "Search system folders", "Search hidden files and folders" and "Search sub folders" can be checked to filter all the files through which can able to spread (This is applicable for Windows XP).

The executable files, information files and html files will be filtered and displayed in the search window. Now by deleting all the files, virus will get removed. This has to be done each and every time the external storage devices got used in other computers. Unexpectedly a non infected software setup files and wanted html files will also get deleted. To avoid this inconvenience, we must avoid storing software and html files in storage devices unnecessarily. If it is compulsory to carry a software of html file through external storage devices, then follow the below said two solutions;

a. Rename the file using dos prompt by executing the "ren" command with parameter "*.exe *.avi", "*.html *.av2" and "*.htm *.av3" one by one. Now the files will change their extensions. For example the file name "abc.exe" may change as "abc.avi". By doing this two benefits will occur. One is the virus will think that file as a non executable file and may not try or infect it. Second, during the search process as said above, the file will not get filtered and deleted manually. Whenever it needs to be used it has to be renamed to its original extension.

b. All the necessary executable, html and information files should be grouped as an ISO disk image. That is the necessary files has to be written using Nero like burning software and instead of writing it in the original disk, it has to be written using image recorder for creating CD/DVD image files (Either in nrg format or in ISO format). Now all the required files will be stored in a single disk image file. These files are safer to copy in the external storage devices, since the virus may not able to alter these image files easily. To get the software and html files back from the ISO image file, the tools like "Nero ImageDrive" can be used.

The above said solutions will decrease the chance of virus spread from external storage device. This solution may be useful for the home users and mobile users.

Preventing virus infection from network connectivity:

The automatic virus spread from network can be minimized by using proper firewall settings. The exceptions should not be allowed unnecessarily in the firewall setting and exactly few port numbers which is required to access required services from the network has to be enabled. The unknown ports belongs to the unwanted services have to be blocked. The virus which spreads by the web pages can be prevented by using the setting available in the internet options of the web browsers. By blocking the activex controls and plug-ins from the internet may minimize the chances of virus spreading. The script execution has to be blocked. But, blocking all these things may affect the browsing process, many services may not be available to user and many part of the web page may not be displayed properly. To overcome this problem, the above said settings should not be applied for trusted sites. For trusted sites we can enable the activex controls and plug-ins. At the time of accessing the emails, the attachments should not be opened if it is not from trusted sender, since some type of virus will spread through emails.

SYSTEM MAINTENANCE

The above said solutions will reduce the virus infection, but it will not give 100% protection to our system. Because the user may not follow the solutions at all time. By mistake if the user opens the virus file, then the infection will start. So

the users must be aware of system maintenance and recovery. Normally, when the system gets crashed, the user will format the hard disk and go for reinstallation of operating systems, driver and other required software. This will take too much of time and effort. At the time of reinstallation, all the required CD/DVD should available. To avoid this inconvenience, proper backup of the system has to be taken for future recovery.

When and how to take the backup?:

Before creating a backup file, the system has to be formatted properly to remove the viruses completely. After formatting, the operating system has to be installed using original disk. Then the required hardware drives and software should be installed using original CDs/DVDs. The required settings like firewall setting, browser setting and registry setting has be done before using the external storage devices and network connectivity to ensure the absence of virus. In this stage the backup can be created using the tools like "Ghost". The "Ghost" software can execute in the DOS operating system. To use the ghost software a bootable disk should be created with DOS operating system. Then the system should be restarted using boot disk and DOS operating should be loaded for executing ghost like software. Using the ghost software the content of C drive (bootable primary partition) should backup. The backup content can be saved as a single file in any medium.

When to restore the backup file?:

When the system gets crashed due to factors like virus, frequent power failure, unexpected mistakes done by users like deleting, editing and configuring of system files and system instability due to errors in various hardware, the backup file can be used to restore the system. For restoring the system, the bootable disk with DOS operating system has to be used again. Unfortunately, during the restore process all the previous files stored in the c drive (Any restored drive) may be lost. To avoid such data loss, each and every file should be stored in other partitions not in c drive (Partition in which the operating system and other software installed). By doing this the data loss will be avoided. The time taken for the restore process depends on the speed of the system hardware. Comparing the time taken for reinstallation, the restore process will get completed ten times faster. Hence, the restore process can be repeated periodically once in a month or week as needed even if the system is in good condition to maintain the performance.

CONCLUSION

In this paper we have identified the problems created by virus, power failures and user's mistakes and we have suggested few solutions. These suggestions will be helpful for the beginners in preventing virus infections without using antivirus software and to recover their system from crash in short time.

ACKNOWLEDGMENT

Our sincere thanks to our honorable Chairman **Dr.P.Selvam M.A., B.Ed., M.Phil., Ph.D., D.Litt.,** P.S.V. College of Engineering and Technology, Krishnagiri, for giving this opportunity. We express my profound gratefulness to our Principal **Dr.K.Rangasamy M.E., M.B.A., Ph.d.,** P.S.V. College of Engineering and Technology for his continuous encouragement in publishing technical papers.

REFERENCES

[1]. Behrouz A Forouzan , "Cryptography and Network Security", Tata McGraw Hill Education Pvt. Ltd., New Delhi, pp537-565, 2007.

[2]. Leonard adleman. An abstract theory of computer viruses, In Lecture Notes in Computer Science, vol 403, Springer-Verlag, 1990.

[3]. Christopher V.Feudo. The Computer VirusDesk Reference. Business One Irwin, Homewood. IL, 1992.

[4]. M.Stamp, information Security: Principles and practice, August 2005.

[5]. Peter J.Denning, editor. Computers under Attack: Intruders, Worms and Viruses. ACMPress, 1990.

