Review Article | Impact Factor: 0.621 | ISSN: 2319-507X
Parag Deshmukh, IJPRET, 2014; Volume 2 (9): 968-973 | IJPRET

INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

VIRUSES HEADACHE TO IT WORLD

MR. PARAG S. DESHMUKH[1], Dr. H. R. DESHMUKH[2], R. G. ANANTWAR[3], R. N. GADBAIL[3]

1. M. E. First Year, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
2. Prof and HOD, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.
3. Asst. Prof, Department of Computer Science & Engineering, IBSS College of Engineering, Amravati.

Accepted Date: 27/02/2014 ; Published Date: 01/05/2014

Abstract: Firstly this is a review paper of types of viruses and their impact on IT world. A virus is by definition a computer program that spreads or replicates by copying itself. The term virus covers a wide range of computer programs that have one thing in common. Once released, they replicate in a way that cannot be controlled by their author. This can easily, intentionally or unintentionally, lead to worldwide epidemics where millions of computers may become infected. The purpose of this paper is to shed some light on viruses, how they work those results in headache to IT world. However, this paper does not cover virus prevention and scanning techniques. All kinds of personal computers such as PCs, Macintoshes etc. and handheld computers, such as Palm, Psion and Pocket-PC, are actually suitable environments for viruses. The virus problem, however, is worst in the PC environment. Both the number of known viruses and the likelihood of being infected is by far the highest in this environment. For that reason, only PC viruses will be covered in this paper.

Keywords: 32-bit viruses, Boot sector viruses, Document viruses, File viruses, Traditional file viruses

PAPER-QR CODE

Corresponding Author: MR. PARAG S. DESHMUKH

Access Online On:

www.ijpret.com

How to Cite This Article:

Parag Deshmukh, IJPRET, 2014; Volume 2 (9): 968-973

INTRODUCTION

A virus is a program that can replicates itself and pass on malicious code to other non-malicious program by modifying them .The term virus was coined because the affected program acts like a biological virus: It infects other healthy subjects by attaching itself to a program and either destroying it or coexisting with it. Because viruses are insidious, we cannot assume that a clean program yesterday is still clean today. Moreover a good program can be modified to include a copy of the virus program, so infected good program itself begins to act as a virus, infecting other program. A virus can be either transient or resident. A transient virus has a life that depends on the life of its host: the virus runs when its attached program executes and terminates when its attached program ends. A resident virus locates itself in memory; then it can remain active or be activated as stand-alone program, even after its attached programs end.

TYPES OF VIRUSES

Boot sector viruses

A boot sector virus infects the boot sector of floppy disks or hard drives. These blocks contain a small computer program that participates in starting the computer. A virus can infect the system by replacing or attaching itself to these blocks. These viruses replicate very slowly because they can only travel from one computer to another on a diskette. In addition, a boot attempt must be made on the target computer using the infected diskette before the virus can infect it. The virus may, however, reside on the diskette and infect new computers even if there is no operating system on it. Network communications have replaced diskettes as a means of sharing data. Software is also distributed using networks or CD-ROMs rather than diskettes. This has made the boot sector viruses almost extinct. Some boot sector viruses still remain on stored diskettes, but they are rarely activated and usually do not work in modern operating systems. However, some damage does occur because these viruses may unintentionally damage file systems that they do not understand.

Traditional file viruses

This group of viruses replicates when attached to MS-DOS program files with the EXE or COM extensions. They cannot infect 32-bit EXE files used by newer versions of MS Windows. This group of viruses can replicate over any media that can transfer files, such as diskettes, local area networks, remote lines etc. Email did not play a significant role in spreading these viruses, as it was an unusual way of communicating in MS-DOS and Windows 3.x-based environments. These viruses, however, have a clear disadvantage compared to boot sector viruses; they

require that program files be transmitted. In business environments this is usually done only as part of a maintenance procedure, not as part of everyday computer usage. Home users writing their own computer programs provide a much better environment for file viruses. This group of viruses is extinct due to the fact that they rely on operating systems that are no longer used.

Document or macro viruses

Document or macro viruses are written in a macro language. Such languages are usually included in advanced applications such as word processing and spreadsheet programs. The vast majority of known macro viruses replicate using the MS Office program suite, mainly MS Word and MS Excel, but some viruses targeting other applications are known as well. Documents created using these applications are actually quite complex container files. The files work internally like miniature file systems. Separate so called "data streams" are created for the actual document data, data saved for undo operations, revisions of the document, embedded objects, macro procedures etc. It is usually easy for a virus to add its macros to the file using the application's own functions. High-level interfaces are available and the virus author does not need to understand how the macros are stored. The macro systems of these applications usually include features that make it possible to run certain macros automatically when a document is opened. Viruses use these features to activate when the virus is copied to a new computer. Macro viruses differ from earlier boot sector and file viruses in many ways. Most differences are beneficial to macro viruses and enable them to spread much faster than any other kind of virus seen thus far. The most important difference is that macro viruses infect data files rather than program files. This takes advantage of a computer environment in a much more efficient way than previous virus types. It is clear that a virus that infects data files rather than program files spreads much more efficiently. Another factor that enabled macro viruses to spread even faster was the fact that email was becoming popular in large corporations at the same time. A clear trend could be seen at that time, as multinational companies that used email heavily internally suffered from the most severe macro virus epidemics. Most macro viruses also contain the virus code in readable source format. Previous virus types were written in low-level languages and compiled into machine code format. This made them unreadable for humans without special tools and advanced programming skills. The ability to read, understand and even modify the virus code produced numerous variants of the widespread macro viruses.

32-bit file viruses

A new group of file viruses emerged as the 32-bit operating systems became more popular. These viruses are by nature similar to the previous file viruses with the exception that they can infect the new file format and work in 32-bit environments. This category is also called PE-

viruses, because the new executable file format's name is PE (portable executable). The new format is also used by many other modules in the system, such as DLLs, system drivers etc. Some viruses infect these modules as well, but most stick to program files with the EXE extension. The number of known 32-bit file viruses is rather small. The most probable reason is that the new file format is complex and making a virus that infects these files is significantly harder than making other types of viruses. This type of virus has become widespread mainly among home users who tend to exchange program files more frequently than business users.

IMPACT ON IT SYSTEMS

The damage caused by viruses can be divided into two categories: intentional damage and unintentional damage. Intentional damage, or harmless effects, is caused explicitly by the payload routine. Unintentional damage may be caused as a side effect when the virus replicates. It is a common misconception that all viruses are malicious by nature. As a matter of fact, many common viruses lack a payload altogether. It is natural that a virus that does not harm its hosts spreads much more efficiently than a destructive virus. The virus is dependent on the host and harming it also reduces the virus' chances to replicate. The term harmless virus is sometimes used to describe a virus that lacks a payload routine, or has a payload routine that only contains non-malicious effects. However, this term is misleading as most viruses are likely to cause some kind of unintentional damage. Many viruses also contain a single or multiple intentional effects.

Harmless effects

These effects are always produced by the payload routine, but they are not malicious. The effect may be a picture, animations or video, music or sounds, interactive functions, political messages etc. These effects usually give you an idea about the virus author's way of thinking, age or nationality. These effects may be funny or annoying and may distract or disturb the user, but they do not cause any permanent damage.

Compatibility problems

Individuals make viruses do not have resources to test their creations on a wide range of computer systems. Nor do they develop the viruses according to quality control systems and guidelines. This makes it likely that they cause compatibility problems when run on systems that differ from the one on which they were developed. These problems can occur as error messages, crashes, inability to access certain functions etc. These problems are grouped as unintentional damage.

Compromising system integrity

Intentional damage is often caused by erasure or modification of data. Erasing files is perhaps the most obvious way to cause damage. Erasing files, however, is a clumsy way and modern, well maintained, systems can usually recover from backups. Modifying data is a much more sophisticated strategy. Small changes are made to the system now and then. The backup routine stores partially corrupted data until the virus is detected. Restoring the data is hard or impossible as several generations of backups are compromised. The last correct backups may be too old and it may even be hard to tell which backups are or are not valid. High-level viruses, such as macro viruses, do not have to operate on binary data as previous viruses did. The macro languages provide powerful functions for modifying data in documents. This enables viruses to perform sinister modifications that are critical but hard to detect. For example, it is possible for a macro virus to alter the text of a document before printing, but show the correct form on screen. Usage of corrupted data may lead to severe damage. An Excel sheet may, for example, be used to calculate the amount of concrete needed for a bridge, or calculate how much fuel a jumbo jet needs to cross the Pacific.

Granting unauthorized access

Viruses may plant backdoors in the system, or steal passwords. These functions can later be used by hackers to access the system. Damage caused by such hacking activities is hard to predict. Unauthorized usage of the system may, for example, continue unnoticed for a long time.

Disclosure of confidential data

Viruses have access to the same communication methods as the user, and even use them to replicate. A payload routine may easily locate documents that match certain criteria and send them to anyone on the Internet.

Computer resource usage

Viruses can disturb computer systems by spending resources, either intentionally or unintentionally. Some viruses contain payloads that deliberately eat system resources, but resource consumption is probably unintentional in most cases. Unintentional resource consumption may be caused by errors in the virus or the replication. Code Red is an example of this. Searching for new hosts to spread to requires both network traffic and CPU resources. This load was obvious in the slower response time from the infected web servers or even in the total inability to serve users. Another type of intentional resource usage is known as denial-of-service or DOS. This is typically performed using distributed technology where a large number of

computers run so-called 'zombies'. All these zombies are programmed to connect to the same computer simultaneously. This does not significantly harm the systems that run the zombies, but the target system is usually blocked due to an overloaded Internet connection.

Human resource usage

Cleaning virus infections means extra work for the IT support staff. This damage, and the downtime for the user, may result in great expense unless the viruses are stopped properly using anti-virus software. Even if viruses are successfully stopped using anti-virus software, the cost of maintaining this system may be seen as a cost caused by viruses.

CONCLUSION

In this paper, different viruses in the computer system and their impact on IT sector are surveyed. It is concluded that viruses attacks specific file types and manipulates a program to execute tasks unintentionally. Also the intentional virus attacks on IT world can be increases day by day that results in above mentioned problems.

REFERENCES

1. Charles P. Pfleeger, Shari Lawrence Pfleeger and Deven Shah, Security in Computing, 4th edition Prentice-Hall, Inc., 2007.

2. http://www.bbox.ch/Beilagen/virus.pdf

3. P. Szor, The Art of Computer Virus Research and Defense. Addison Wesley, (2005)

4. http://www.emis.de/journals/IJOPCM/files/IJOPCM(vol.1.2.3.S.08).pdf

5. http://www2.bgsu.edu/downloads/cio/file17753.pdf

6. http://my.safaribooksonline.com/book/networking/security/0132390779.