Computer Viruses

Sachin Dnyandeo Ubarhande

Research Scholar, Department of Software Systems
RGPV University, Bhopal, India

Abstract— While technology advances have brought many benefits to society there have also been technological abuses .In today's generation, with the help of the Internet and the rapid growth of the personal computer in the average household, we are able to talk to and share information with people from all sides of the globe .Unfortunately this transformation of data has opened the doors for a new era of high tech crime - the computer virus. The Internet is now a complex gateway for transgression and immoral activities where often the perpetrators of the crime are far removed from the scene of the criminal activity and hidden behind maze of double speak. Today a properly engineered virus can have a devastating effect on the Worldwide Internet showing just how sophisticated and interconnected human beings have become. For example, the Melissa Virus, which became a global phenomenon in March 1999, was so powerful that it forced Microsoft and a number of other very large companies to completely turn off their e-mail systems until the virus could be contained. Viruses have also provided a weapon for those members of society who wish to harm others for a variety of reasons. As technology is proceeding, programmers are recurrently creating virus shielding software with live updates and enhanced fortification for the most recent viruses. However, the virus protection software’s can not always offer 100 percent protection from all the dangerous and insecure material on the Internet. In conclusion, we can only be assiduous in our use of the World Wide Web and hope to turn clear from these perilous prevailing vulnerabilities.

Index Terms— Introduction,The Basics of the Computer Viruses,Types of Computer Viruses,Functional elements of Virus,Computer Viruss writers,To which extend Computer Viruses writes, make consideration to ethics?,Pro-Active approaches to controlling Viruses.

1 Introduction

The paper will teach you the Basics of the Computer Virus, Types Of Computer Viruses, the Functional Elements of a Virus, Computer Viruses Writers and how Can Home Users eliminate The Threat Of Computer Viruses?, Proactive Approaches to Controlling the Viruses. I am convinced that computer viruses are not evil and that programmers have a right to create them, posses them and experiment with them. That kind of a stand is going to offend a lot of people, no matter how it is presented. Even a purely technical treatment of viruses which simply discussed how to write them and provided some examples would be offensive. The mere thought of a million well armed hackers out there is enough to drive some bureaucrats mad. This paper goes beyond a technical treatment, though, to defend the idea that viruses can be useful, interesting, and just plain fun. That is bound to prove even more offensive. Still, the truth is the truth, and it needs to be spoken, even if it is offensive. Morals and ethics cannot be determined by a majority vote, any more than they can be determined by the barrel of a gun or a loud mouth.. As long as computers have been around, men have dreamed of intelligent machines which would reason, and act without being told step by step just what to do. For many years this was purely science fiction. However, the very thought of this possibility drove some to attempt to make it a reality. Thus “artificial intelligence” was born. Yet AI applications are often driven by commercial interests, and tend to be colored by that fact. Typical results are knowledge bases

and the like—useful, sometimes exciting, but also geared toward putting the machine to use in a specific way, rather than to exploring it on its own terms. The computer virus is a radical new approach to this idea of “living machines.”

2 The Basics Of The Computer Virus

The essential feature of a computer program that causes it to be classified as a virus is not its ability to destroy data, but its ability to gain control of the computer and make a fully functional copy of itself. It can reproduce. When it is executed, it makes one or more copies of itself. Those copies may later be executed, to create still more copies, ad infinitum. Not all computer programs that are destructive are classified as viruses because they do not all reproduce, and not all viruses are destructive because reproduction is not destructive. However, all viruses do reproduce. The idea that computer viruses are always destructive is deeply ingrained in most people's thinking though. The very term "virus" is an inaccurate and emotionally charged epithet. The scientifically correct term for a computer virus is "self-reproducing automaton or "SRA" for short. This term describes correctly what such a program does, rather than attaching emotional energy to it. Among the most sophisticated of computer programmers, the computer virus is the vehicle of choice for deploying destructive code. A computer virus has the same two goals as a living organism: to survive and to reproduce. The simplest of living organisms depend only on the inanimate, inorganic environment for what they need to achieve their goals. They draw raw materials from their surroundings, and use energy from the sun to synthesize whatever chemicals they need to do the job. The organism is not dependent on another form of life which it must somehow eat, or attack to continue its existence. In the same way, a computer virus uses the computer system's resources like disk storage and CPU time to achieve its goals. Specifically, it does not attack other self-reproducing automata and "eat" them in a manner similar to a biological virus.

3 Types Of Computer Viruses

Every year computers technology developers surprise the world with their new inventions, therefore virus writers need to create new generations of viruses to cope with the latest computing techniques. As a result of this competition each year hundreds of new viruses are found in the wild.

3.1 File-infecting virus

This virus technique is to attach itself to the executable files, which are the files ending with .exe, .com, .all, and .drv , and these are the main program files and drivers. If any of them is infected the virus code will be executed during the run first by loading itself to the memory and deceive the user by allowing the program to execute normally. When the user runs any other applications, the virus replicates itself in order to be attached to that application. The virus should remain undetected until trigger is reached and this depends on the virus writer choices.

3.2 Boot sector virus

This virus loads itself to the boot sector of the floppy disk or master record of hard disk in order to be loaded to the memory before the operating system is loaded. As soon as the virus becomes residence it will be able to infect each inserted disk to that computer.

3.3 Macro viruses

The macro language technology was invented by software companies in order to automate repetitive tasks. This virus depends on the macro language in order to infect the data files by attaching themselves to the global template and spreads when the data files are opened. So as we can see virus writers took advantage of a new invention and developed a stabile virus for each age. These types of viruses are categorized as dangerous ones, because they are easy to write, spread easily, and its hard to eradicate them. The macro virus's effect could be an annoying massage, adding password protection to files, saving files as templates instead of saving them as documents, or moving and replacing the text randomly.

3.3 Script virus

This type of virus is written using script languages, they spread and infect files by taking advantage of vulnerabilities in the Microsoft Windows operating systems; opening e-mails or accessing Web pages which includes tainted scripts will activate the virus. This type of viruses has the ability to change its signature each time the virus is reproduced in order to remain undetected by antivirus software.

3.3 Polymorphic virus

This virus has the ability to change each time it replicates using different encryption routines through its additional unique mutation engine. As a result of this invented combination the virus is very difficult to detect. One Half is an example of this virus, it has a distractive effect, its target is to encrypt the hard disk and make it unreadable. Virus writers are so keen to cope with the technology development, each time antivirus software and software developers come up with a new technology to prevent computer viruses infection, virus writers find their way to surprise the world with a new threat by releasing the suitable virus for each age..

4 Functional Elements Of Virus

Every viable computer virus must have at least two basic parts, or subroutines, if it is even to be called a virus. Firstly, it must contain a search routine, which locates new files or new areas on disk which are worthwhile targets for infection. This routine will determine how well the virus reproduces, e.g., whether it does so quickly or slowly, whether it can infect multiple disks or a single disk, and whether it can infect every portion of a disk or just certain specific areas. As with all programs, there is a size versus functionality tradeoff here. The more sophisticated the search routine is, the more space it will take up. So although an efficient search routine may help a virus to spread faster, it will make the virus bigger, and that is not always so good.Secondly, every computer virus must contain a routine to copy itself into the area which the search routine locates. The copy routine will only be sophisticated enough to do its job without getting caught. The smaller it is, the better. How small it can be will depend on how complex a virus it must copy. For example, a virus which infects only COM files can get by with a much smaller copy routine than a virus which infects EXE files. This is because the EXE file structure is much more complex, so the virus simply needs to do more to attach itself to an EXE file. While the virus only needs to be able to locate suitable hosts and attach itself to them, it is usually helpful to incorporate some additional features into the virus to avoid detection, either by the computer user, or by commercial virus detection software. Anti-detection routines can either be a part of the search or copy routines, or functionally separate from them. For example, the search routine may be severely limited in scope to avoid detection. A routine which checked every file on every disk drive, without limit, would take a long time and cause enough unusual disk activity that an alert user might become suspicious.Alternatively, an antidetection routine might cause the virus to activate under certain special conditions. For example, it might activate only after a certain date has passed (so the virus could lie dormant for a time).

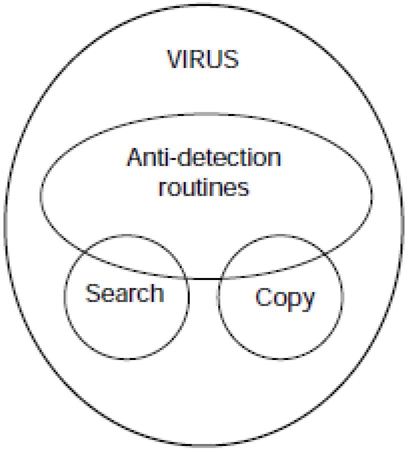

Figure 1: Functional diagram of a virus.

Alternatively, it might activate only if a key has not been pressed for five minutes (suggesting that the user was not there watching his computer). Search, copy, and anti-detection routines are the only necessary components of a computer virus, and they are the components which we will concentrate on in this volume. Of course, many computer viruses have other routines added in on top of the basic three to stop normal computer operation, to cause destruction, or to play practical jokes. Such routines may give the virus character, but they are not essential to its existence. In fact, such routines are usually very detrimental to the virus' goal of survival and self-reproduction, because they make the fact of the virus' existence known to everybody. If there is just a little more disk activity than expected, no one will probably notice, and the virus will go on its merry way. On the other hand, if the screen to one's favorite program comes up saying "Ha! Gotcha!" and then the whole computer locks up, with everything on it ruined, most anyone can figure out that they've been the victim of a destructive program. And if they're smart, they'll get expert help to eradicate it right away. The result is that the viruses on that particular system are killed off, either by themselves or by the clean up crew. Although it may be the case that anything which is not essential to a virus survival may prove detrimental, many computer viruses are written primarily to be smart delivery systems of these "other routines." The virus gets killed in action when its logic bomb goes off, so long as the bomb gets deployed effectively. The virus then becomes just like a Kamikaze pilot, who gives his life to accomplish the mission. Some of these "other routines" have proven to be quite creative. For example, one well known virus turns a computer into a simulation of a wash machine, complete with graphics and sound. Another makes Friday the 13th truly a bad day by coming to life only on that day and destroying data. The situation is similar to having an atomic bomb, but not the means to send it half way around the world in fifteen minutes. Sure, you can deploy it, but crossing borders, getting close to the target, and hiding the bomb all pose considerable risks.

5 Computer Viruses Writers

5.1 The Adolescent

Their age is between 13 and 17 , they should have written one computer virus at least, should have released at least one computer virus to the wild.

5.2 The College Student

Their age is between 18 and 24 , they should have written one computer virus at least, should have released at least one computer virus to the wild. They should be students at university or studying classes at university level.

5.3 The Adult/Professionally Employed

They could be post-college or adults, professionally employed, they should have written one computer virus at least, should have release at least one computer virus to the wild.

5.4 The Ex-Virus Writer

They should have written and released one or more computer viruses. Their viruses should have been found in the wild; they have to prove that they have not written or continued to write viruses for the last 6 months. The previous categorizations depend on the age and education level. To classify virus writers in different groups in order to understand them and know more about their motivations to write and distribute computer viruses in to the wild.

6 To Which Extent Computer Viruses Writers Make Consideration To Ehics?

The observation shows that the virus writers are not a homogenous group, since they vary in age, education level, economical level, background, manner of communication, perspective of their society, and have different preferences. All of the foregoing will lead to different modes of thinking and different motivations behind their behavior. The adolescent and college virus writers are within the norms of their age group of the ethical development model, the reason for their behavior in writing and releasing viruses were unclear according to the collected information, and 'The Enemy' seems to be virtual one. While adult virus writers seem to be under the norm for their age group of the ethical development model.

7 Pro-Active Approaches To Controlling Viruses

Home users are not a homogeneous group, since they are from different ages, backgrounds, education levels, and computing experiences, this is the case in almost all homes. Unfortunately this non homogenous group usually shares the same computer. All family members should practice save computing in order to eliminate the threat of computer viruses. To accomplish this goal home users have to know their enemy by increasing their knowledge about computer viruses, antivirus software, firewalls, practice save computing, getting answers from security sites (e.g., Symantic.com, Quickheal.com), and finally take all the security cautions to protect their systems. "Computer users and systems managers must ensure that their computer systems are secured and that basic IT security principles are followed.

8 Acknowledgment

The completion of the research paper on "Computer Viruses" has given me profound knowledge. I am sincerely thankful to Prof.Hitesh Gupta [Head of Department M.Tech Software Systems,PGOI, Bhopal] and Prof.Mukesh Kumar Baghel to get valued depth knowledge during the preparation of this research paper and also to Mark A. Ludwig -Author of Black Book of Computer Viruses. My sincere thanks to all.

References

[1] Mark A. Ludwig- Black Book of Computer Viruses.
[2] http://www.quickheal.co.in
[3] http://www.symantec.com
[4] http://www.howstuffworks.com/virus.htm
[5] http://en.wikipedia.org/wiki/Computer_virus