www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 3 Issue 2 February , 2014 Page No. 3869-3872

Computer Viruses and Challenges for Anti-virus Industry

Deepak Kumar[1], Narender Kumar[2], Aditya Kumar[3]

[1]YMCA University of Science & Technology,
Sector 6, Faridabad, Haryana 121006, India
deepakjanghu018@gmail.com

[2]Guru Jambheshwar University of Science & Technology,
Hisar, Haryana 125001, India
narenderster@gmail.com

[3]YMCA University of Science & Technology,
Sector 6, Faridabad, Haryana 121006, India
ymca.aditya@gmail.com

Abstract: ***In today's world every organizations and individuals using computer and internet need to have a wide-ranging virus protection policy to combat the growing threats of computer viruses by means of anti-virus. The anti-virus approach consists of waiting for a number of computers to be infected, detecting the virus, designing a solution, and delivering and deploying the solution. In this situation, it is very difficult to prevent every machine from being compromised by virus. This paper highlights the most common virus types and their modus operandi. Further it is also discussed that in present scenario due to the evolution of new viruses every day why it is very difficult for Anti-virus industry to make themselves up-to-date each day as per the definition of new emerging viruses.***

Keywords: Botnets, Denial of service, Malware, Multipartite virus, Prepending virus, Macro virus, Metamorphic Virus, Antivirus, Metamorphic Virus, Code obfuscation Virus Detection Methods (VDM).

1. Introduction

In comparison of early 90's where the number of known computer viruses was about 1,000 to 2,300 viruses, today this number is escalated to more than 1,00,000. Studies and researches show that a computer connected to the Internet may experience an attack every 39 seconds. The new exposed problems are fixed by the software vendors who provide patches and updates for the system. In the mean time, hackers take advantage of this situation as malicious programs are installed on user machines which steal secret data and provide it to unauthorized person for financial and other types of gains. The contaminated machines can also be made a part of a huge botnets which are groups of computers infected with malicious code and unknowingly controlled by a malicious master. These systems can be used to launch Denial of Service attacks on servers, or be used in an attempt to intrude the computers of government agencies.

2. Computer virus types and strategies

A computer virus is a malware, when executed, try to replicate itself into other executable code; when it succeeds, the code is said to be infected. The infected code, when run, can infect new code in turn. The self-replication into existing executable code is the key defining characteristic of virus. So it is the program that can copy itself and infects a computer without permission or knowledge of the user. Computer virus writers exercise different strategies to avoid detection by anti-virus. Some of the virus types and the associated strategies are –

• **Overwriting Virus:** This type of virus use to overwrite files with their own copy. This is a very primitive and easiest technique. If a user does not spot the infection in time, an overwriting virus can inflict irreversible damage to numerous files.

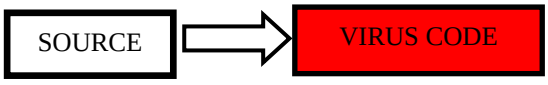


Figure 1

A system that has been compromised by this type of infection can easily become unstable and eventually inoperable. The only solution after infection is to delete the file from the disk. These virus have been known to exploit a wide range of operating systems including Linux, Macintosh, Windows and DOS platforms. Some well-known overwriting viruses are Grog.377,Grog.202/456, Loveletter

• **Companion Infection or Spawning virus or Cluster virus:** Instead of modifying the existing files in a system like most viruses, it creates new ones and sends them off to spread the malicious code. The companion virus works by seeking all files with extensions ending in .EXE. It then creates a matching file that ends in the .COM extension, which is specifically reserved for the malicious code. When the victim attempts to launch an .EXE program, he or she usually types its

name without the extension. In such cases, Windows gives priority to a file with the .COM extension over a file with the same base name. e.g .Globe Virus

• **Appending Virus:** In this virus generating technique, a jump (JMP) instruction is inserted at the front of the host to point to the end of the original host. The appender technique can be implemented for any other type of executable file, such as .EXE, .ELF etc. extensions, and so on.

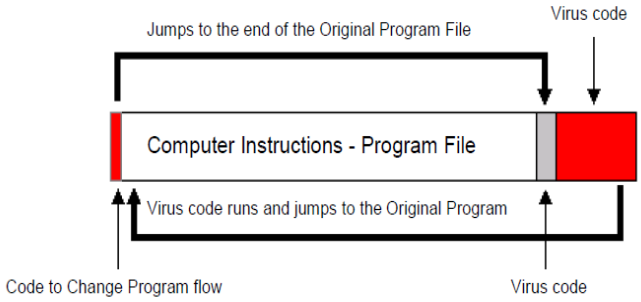


Figure 2

Such files have stores the address of the main entry point in the file header, which, in most cases, will be replaced with a new entry point to the start of the virus code appended to the end of the file so that to ensure that the commands contained in the virus code are executed before infected object commands. A typical example of this virus is Vienna.

• **Prepending Virus:** This virus inserts its code at the front of host programs. This is a simple kind of infection, and it is often very successful. Virus writers have implemented it on various operating systems.

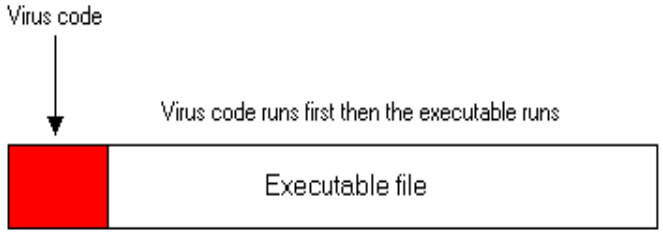


Figure 3

In general, this virus prepends itself, some bytes long, at the front of the executable and shifts the original program content to follow itself. An example of a prepender virus is the Hungarian virus Polimer.512.A.

• **Cavity or spacefiller Virus:** This virus attempts to install itself in this empty space while not damaging the actual program itself. Actually, some program files, for a number of reasons, have empty space inside of them. This empty space can be used to house virus code.

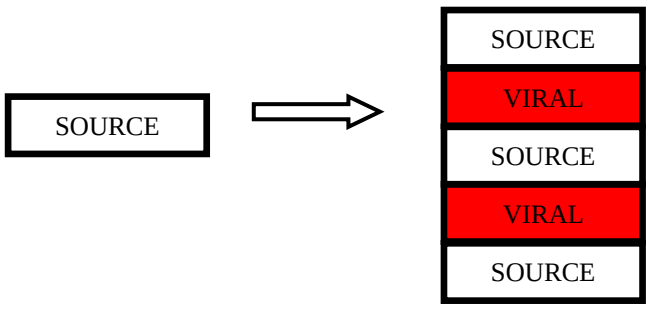


Figure 4

A spacefiller virus attempts to install itself in this empty space while not damaging the actual program itself. An advantage of this is that the virus then does not increase the length of the program. Because of the difficulty of writing this type of virus and the limited number of possible hosts, cavity viruses are rare. The Lehigh virus was an early example of a cavity virus.

• **Boot Sectors Virus:** Boot sector is that area of the computer that is accessed when the computer is turned on. A boot sector virus infects this portion. Once the boot sector is infected the virus is loaded into memory when the computer is turned on. This virus then infects boot sectors on floppies or other removable media Master Boot record virus only infects the Master boot record and not the boot sector.

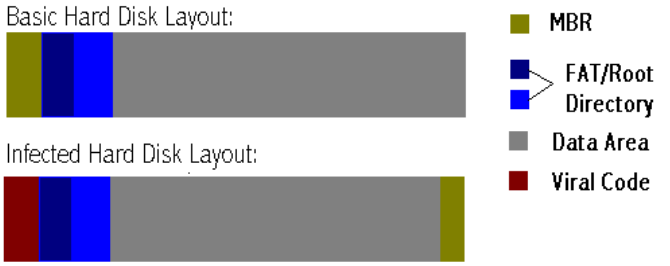


Figure 5

Boot sector viruses gain complete control of the master boot record or the DOS boot sector by replacing the operating system contents with that of its own. This allows the virus to spread fast and cause damages like to redirect disk reads, moving or damaging the master boot record to another location causing the system to crash when it boots up or to corrupt the File Allocation Table (FAT) which is the index of all the files on the drive. Michelangelo virus is an example of a Boot Sectors Virus. Generally this type of message is shown after the attack of boot sector virus:

```
Non system-disk or disk error.
Replace and strike any key when
ready.
```

Figure 6

• **Macro virus:** This type infects a Microsoft Word Documents, Excel Spreadsheets, Power point presentations, and Access Databases or similar applications and causes a sequence of actions to be performed automatically when the application is started or something else triggers it. Macro Viruses uses the macro language for its program. Microsoft office has got the macro language built into its application and so most of its application programs are affected by this virus. A macro virus is often spread as an e-mail virus. The Header of e-mail is look like that:

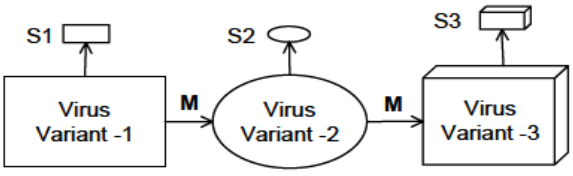
```
Subject: Extremely URGENT: To All E-
Mail User - <current date>

Attachment: <Infected Active
Document>

Body: This announcement is for all
E-MAIL user. Please take
      note that our E-Mail Server
will down and we recommended
      you to read the document which
attached with this E-Mail.
```

Figure 7

A well-known example was the Melissa email virus. Script viruses are other form of Macro Virus that are mobile codes, downloaded from a remote system and executed locally with minimal or no user intervention. Java applets, JavaScript scripts, Visual Basic Scripts (VBScripts), and ActiveX controls are some of the most popular examples of mobile code that may encounter while browsing the Web or reading HTML-formatted e-mail. An attacker might use mobile code for a variety of nasty activities, including monitoring your browsing activities, obtaining unauthorized access to your file system, infecting your machine with a Trojan horse, hijacking Web browser to visit sites that one did not intend to visit, etc. .

• **Multipartite Virus:** This virus combines the characteristics of more than one type of viruses thus acting as hybrid virus which gives it the ability to infect boot system sectors as well as program files. It often infects the section on a hard drive that contains data which instructs the machine on how to boot up. Whenever the computer starts, the virus is automatically distributed throughout the system. This enables it to spread and infect program files, causing a user to unknowingly invoke the virus, resulting in more destructive payloads being delivered into the system. Ghostball, is the example of first multipartite virus.

• **Metamorphic Virus:** Metamorphic Virus can reprogram itself with each infection while maintaining the same functionality. It uses code obfuscation techniques to challenge deeper static analysis and can also defend itself from dynamic analyzers of anti-virus by altering its behavior.



Legend

M – Morphing transformations
{S1, S2, S3} – Virus Signatures

Figure 8

It does this by translating its own code into a temporary representation, edit the temporary representation of itself, and then write itself back to normal code again. This is intended to avoid detection by anti-malware software, but can usually be overcome via emulation or other techniques, and in many cases is deployed in a flawed manner leading to large numbers of misinfections.

Metamorphic viruses use several metamorphic transformations, including Instruction reordering, data reordering, inlining and outlining, register renaming, code permutation, code expansion, code shrinking, Subroutine interleaving, and garbage code insertion. The altered code is then recompiled to create a virus executable that looks fundamentally different from the original.

3. Challenges for Antivirus Industry

Virus Detection Methods(VDM) have some major problems and for the same reason many anti-virus industries facing one or more troubles out of the following:

• VDMs are only good against known viruses and not very good against evolutionary or new viruses. The number and variety of malicious programs is increasing year on year. The result is that many antivirus companies are simply unable to cope with this situation. Users who chose products manufactured by such companies will not be protected against all malicious programs. It is so because different anti-virus companies may or may not have the definitions or signatures of all the viruses in their database.

• Metamorphic viruses are difficult to detect because their creators have the advantage of knowing the weaknesses of antivirus scanners. The limits of antivirus scanners come from the limits of static and dynamic analysis techniques.

• Malicious programs spreads so fast that antivirus companies have to release updates as quickly as possible to minimize the amount of time that users will potentially be at risk. But, many antivirus companies are unable to do this at needful speed.

• Another problem is to delete malicious code detected on the victim machine. Very often viruses and Trojans are written in a way which enables them to hide their presence in the system and/ or to penetrate the system so deeply that deleting them is a complex task and further to restore the data which has been modified by the virus without causing problems.

• All software including the anti-virus uses system resources. In order to

• Protect the computer, the antivirus program has to perform certain actions - open files, read information in them, open archives to scan them etc. . The more thoroughly a file is checked, the more resources and time are required by the antivirus solution. So the problem is balancing program speed against the level of protection provided.

• An additional issue is the incompatibility between antivirus programs. In the vast majority of cases, installing two antivirus programs from different vendors on one machine (for increased protection) is technically impossible, as the two programs will disrupt each other's functioning.

4. Conclusion

Computer viruses have been around almost as long as computers. Computer viruses have dramatically increased in complexity over the years. Latest technical development such as high speed network, internet & advance personal computers have provided viruses a main threat to the computers. A computer virus, a few KBs in size, like any piece of code, which when executed on computer, carries out a particular task, can destroy gigabytes of data stored in computer and bring the biggest organization to a halt. A lot of anti-virus software is available in the market and being widely used but these anti-

viruses are less effective as they are made only for the existing viruses not for the viruses which developed latter These elaborate viruses have placed a strain on anti-virus procedure. As there is no way to implement a totally secure policy but it is necessary to create a strategy and use combined technologies to prevent computer virus. A better understanding of the issues which the antivirus industry faces will help the user when selecting an antivirus solution for home computer or network. Information is the key to survival, and can protect from unpleasant consequences. Most recent statistics indicate that the following simple steps can help control the problem, cutting this figure by more than half by making sure that users use anti-virus software and they know what viruses are and whom to contact if they find one. By and large, the field is by no means complete, and easily anticipated problems in the relatively near future will require substantial new invention to avoid significant problems with new viruses.

References

[1] Mark Ludwig, The Little Black book of Computer Virus, American Eagle Publication.
[2] J. cock, Computer Viruses and Malware, Springer.
[3] Peter Szor, The Art of Computer Virus Research and Defense, Addison Wesley Professional.
[4] Peter Gregory, Computer Virus for Dummies, Wiley Publications
[5] The Norman book on computer viruses.
[6] http://www.cknow.com/vtutor/NumberofViruses.html
[7] http://www.spamlaws.com
[8] http://www.viruslist.com

Author Profile

Deepak Kumar received the B.Tech. Degree in Computer Science & Engineering from Kurukshetra University and M.Tech. Degree in Computer Science & Engineering from M.D. University in 2006 and 2008 respectively. He has qualified for National Eligibility Test (NET)/JRF for teaching in Computer Science & Applications conducted by University Grant Commission (UGC). He has also passed Graduate Aptitude Test in Engineering (GATE) and has been awarded Ministry of Human Resource Development (MHRD) Scholarship. He has also been associated with Ministry of Information & Technology (MIT), New Delhi for 6 months.