International Journal of Scientific & Engineering Research Volume 9, Issue 4, April-2018
ISSN 2229-5518

The Surveillance on Computer Viruses and Its Security

[1]P.BalaKrishnan, [2]G.Ajay

Abstract—today, safety of our data is a big question from various threats come from online and offline. This paper describes about the computer viruses, and how they are stealing the data and destroying the systems. Virus can result in poor performance, loss of data, loopholes in system. Because of it, everyone who uses computers have a fear of losing data. On the other hand, anti-virus technologies are continually followed the virus tricks and methodologies to overcome their threats. So the user wants to know about the knowledge of computer viruses and their prevention tips. This paper shows about viruses briefly and about analysis techniques for user. The beginner should protect their valuable data from these threats using different anti-virus software tools available in market. The development of the computer viruses and their prevention (anti-virus) methods are described here.

Keywords Malware, Virus, Virus Detection Techniques, Antivirus, computer security, Defensive, Virus, Malware, Antivirus.

1 INTRODUCTION

Nowadays, there is a huge variety of cyber threats that can be quite dangerous not only for big user but also for ordinary user, who was a potential victim for cybercriminals when using unsafe computer system for entering into a confidential data, such as login, user name, password, credit card numbers, data threat, etc., [1].Where malicious programs are installed on user machines to steal secret data for financial gains [4]. Virus has evolved into more complex form to prevent its detection. Due to destructive action of virus, its detection has become an important vertical in computer world [5]. The Robert Morris Internet Worm that was released in the fall of 1988 caused a great deal of damage to the Internet [6]. Computer security was the protection of information systems from data theft or damage system to the hardware and software. It is also known as cyber security or IT security [9].

One with the capability to reproduce and the other to transfer instances to other email clients via email addresses found in the initially infected email client. In addition, there is a payload or malicious act that may await a set of predetermined circumstances before being activated or triggered. Viruses remain a significant threat to modern networked computer systems [10]. Over the past 10 years the Internet has become ubiquitous to the average person in the United States. People of all ages use it on a regular basis, and it has become one of the driving forces of the economy. From banking to shopping to communication, it has radically changed the way many people go about their daily lives .Threats for mobile phones, IP-communication threats, social networking threats and even spam. All of these Threats try to violate one of the following criteria: confidentiality, a single Hidden Markov Model (HMM) is used to determine whether a given program belongs to the virus family that the HMM represents.

- [1]*P.Balakrishnan, 2nd MCA, Er.Perumal Manimekalai College of Engineering,Hosur,PH-7708976864,E-mail: bala123505@gmail.com*
- [2]*G.Ajay, 2nd MCA, Er.Perumal Manimekalai college of Engineering,Hosur,PH-9566608981,E-mail: ajayguna1397@gmail.com*

2 THEORY OF COMPUTER VIRUSES

The history begins in 1983, when American scientist Fred Cohen in the dissertation work devoted to research of self-reproducing computer programs for the first time has proposed the term "computer virus" and later on published the article <<Computer Viruses: theory and experiment>> [1].

3 COMPUTER VIRUS

A computer virus is a software program that spreads all over the systems. It was created by a software developer to monitor other's activity and to steal data from other users. The computer viruses can self – replicable programming code to spread all systems.

4 ANTIVIRUS

Antivirus is software to protect our systems from malware, threads, viruses and worms. From installing the software (antivirus) for system it removes the viruses and system problems and the system runs smoothly. But some latest viruses are not identified by antivirus software, Because of upraising the update of computer viruses versions are becoming very strong than the antivirus software.

5 COMPUTER VIRUS TYPES AND STRATEGIES

A computer virus is a software program malware virus, when it executed, it will try to replicate itself into other executable codes; when it succeeds its goal, the system indicates "infected by virus". Some of the virus types and the associated strategies are [7].

5.1 Overwriting Virus

This type of overwriting virus is use to overwrite the other files with its own copy. It is very primitive and very easiest technique. If a user will not find the infection in time, an overwriting virus can inflict irreversible damage to all numerous files.

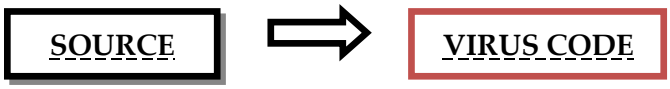

Fig: 1

A system that has been compromised by this type of problem can easily become unstable and inoperable. The only solution, when infection will delete the file from the disk. These viruses 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, Love letter [8].

5.2 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 to spread the malicious code. The companion virus works by seeking all files ending with .EXE extension. Then it creates a matching same file that ends with .COM extension, which is specifically reserved for the malicious code [8].

5.3 Appending Virus

The appending virus is inserted at the front of the host to point to the end of the original host. This appended technique can be implemented for any other types of executable file, such as .EXE, .ELF etc.

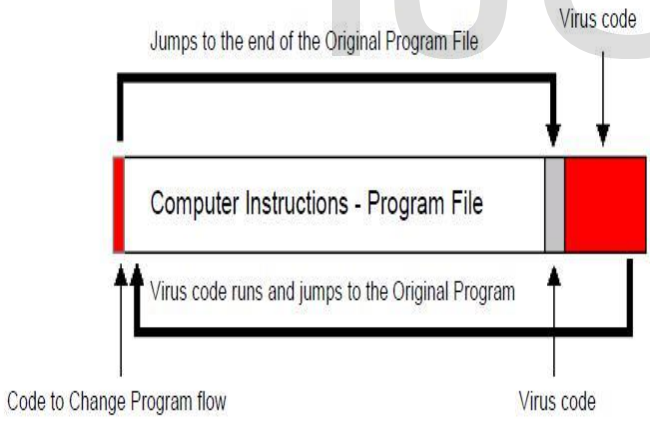

Fig: 2

Such files stores the address of the main entry point in the file header, which, in most cases, it 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 [8].

5.4 Prepending Virus

This prepending virus inserts its code at the front of host programs. This is a simple kind of infection, and it happens very successful. Virus creators have implemented it on different operating systems [8].

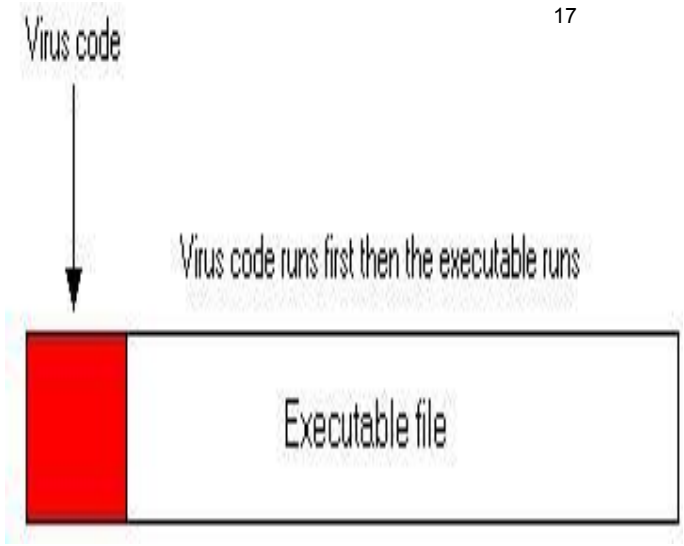

Fig: 3

5.5 Cavity or space filler Virus

This virus attempts to install itself in the empty space while it not damaging the actual programs itself. Actually, some program files, for a number of reasons, have an empty space inside of them. This empty space can be used as like house for virus code.

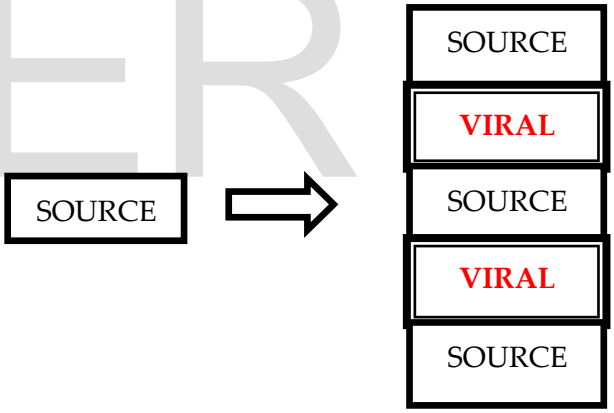

Fig: 4

Advantage of this virus does not increase the length of the program. The Lehigh virus was an early example of a cavity virus [8].

5.6 Boot Sectors Virus

Boot sector is that area of the computer that is accessed when the computer is turned on. A boot sector virus affects this portion. Once the boot sector is infected, it was loaded into memory when the computer is turned on. This virus infects only boot sectors on floppies or other removable media, Master Boot record. This virus only affects the Master boot record and not the boot sector.

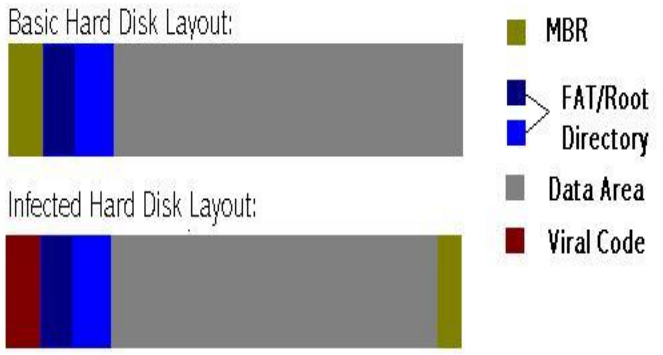

Fig: 5

Boot sector viruses' takes complete control of the master boot record or the DOS boot sector by replacing the operating system contents with 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. Michelangelo virus is an example of a Boot Sectors Virus. Generally this type of message is shown after the attack of boot sector virus [8].

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

Fig: 6

5.7 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. 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 also spread as an e-mail virus. The Header of e-mail is look like that [8].

```
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.
```

Fig: 7

5.8 Metamorphic Virus

Metamorphic Virus can reprogram itself with each infection. And it can maintain the same functionality. It uses most complicate code techniques to challenge deeper static analysis and can also protect itself from dynamic analyzers (anti-virus) by modifying its behavior.

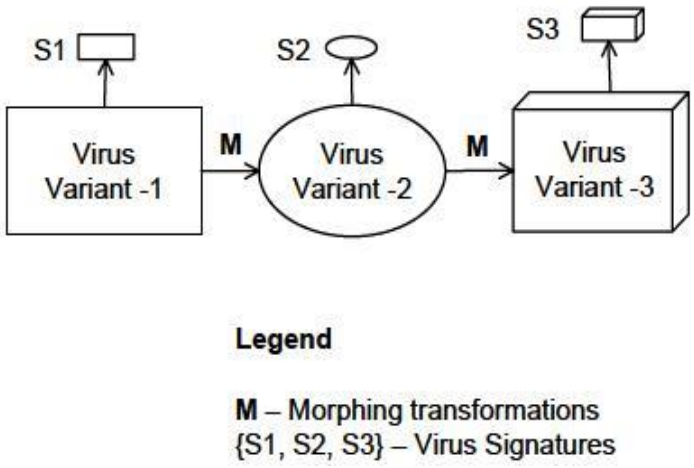

Fig: 8

It can alternate by translating its own code into a temporary representation, after itself edits the temporary representation, and then again writes itself back to a normal code. This work is done to protect itself to escape from anti-malware software [8].

6 Works Done by Computer Viruses

- A virus can be a way for a hacker or programmer to show off his ability.
- A computer virus can be used to steal people's personal information.
- A virus is able to take control of a person's computer.
- Online advertising is often targeted by hackers, who make money from virus-related scams (for example 'click jacking').

7 Preventing from Computer Viruses

- Install Anti-Virus/Malware Software
- Keep Your Anti-Virus Software Up to Date
- Keep Your Operating System Current
- Secure Your Network
- Think before You Click
- Keep Your Personal Information Safe
- Don't Use Open Wi-Fi
- Back Up Your Files

9 Conclusion

In this paper computer viruses are most dangerous programs. So the users want to protect their systems from infecting by the virus programs. By using anti-virus software the user can protect their system from attack of virus. The given information cannot cover all type of

Computer viruses and its anti-virus software programs. So the users are aware from Computer virus and use Anti-virus software's to protect their systems from computer viruses to be able to use the installed protection system effectively.

REFERENCES

[1] Studying and Classification of the Most Significant Malicious Software, Dr. Wajeb GHARIBI, Computer Science & Information Systems College, Jazan University, Jazan, KSA. E-mail: gharibi@jazanu.edu.sa.

[2] The New Age Of Computer Virus And Their Detection, Nitesh Kumar Dixit, Lokesh mishra, Mahendra Singh Charan and Bhabesh Kumar Dey, Department of Electronics and Communication Engineering, BIET, Sikar, Raj., INDIA , E-mail: nitesh20.dixit@gmail.com.

[3] Where computer security meets national security, Helen Nissenbaum, Department of Culture and Communication, New York University, NY, USA, E-mail: helen.nissenbaum@nyu.edu.

[4] Computer Virus Strategies and Detection Methods, Essam Al Daoud, Iqbal H. Jebril and Belal Zaqaibeh, Department of Computer Science, Zarqa Private University, Jordan, E-mail: essamdz@zpu.edu.jo.

[5] Detecting Computer Viruses , Manju Khari, Chetna Bajaj, Assistant Professor in Ambedkar Institute of Advanced Communication Technoloies and Research, E-mail: manjukhari@yahoo.co.in.

[6] The Case for Beneficial Computer Viruses and Worms, Mr. Greg Moorer, Undergraduate Computer Science Student, Department of Computer Science, Mississippi State University, E-mail: gam3@ra.msstate.edu.

[7] Computer Viruses an Introduction, Jeffrey Horton, Department of Computer Science University of Wollongong, North Fields Avenue, Wollongong, E-mail: jeffh@cs.uow.edu.au.

[8] Computer Viruses and Challenges for Anti-virus Industry , Deepak Kumar, Narender Kumar, Aditya Kumar, YMCA University of Science & Technology, Sector 6, Faridabad, Haryana 121006, India. E-mail: deepakjanghu018@gmail.com.

[9] An Analysis of Various Anti-Virus Software Tools Based On Different Effective Parameters, K. Durga Devi, Research Scholar, Dr. K. Mohan Kumar, Research Guide & Head, Rajah Serfoji Government College, Thanjavur, Tamil Nadu – India

[10] A Framework to Detect Novel Computer Viruses via System Calls, A. A. Abimbola, J. M. Munoz and W. J. Buchanan, School of Computing, Napier University, EH10 5DT, Scotland, UK, E-mail: a.abimbola@napier.ac.uk.