International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 1 | ISSN : 2456-3307

# A Comparison study of Computer Virus and Detection Techniques

**Soumen Chakraborty**
Department of Information Technology, MCKV Institute of Engineering, MAKAUT, West Bengal, India
csoumen88@gmail.com

## ABSTRACT

The virus is a kind of program which seriously infects the system, large organizations nowadays have big data to maintain which are spread to various locations in the world. As a result, security is a major issue for all companies nowadays. The data is the ultimate asset for any people nowadays. Which needs various precautions to maintain to keep safe those assets. As there is growing the popularity of various kind of virus like malware,trojan,hackers,adware it is really becoming a challenge to keep the system secure.With the growing popularity of internet in our daily lives, the risk of various kind of threats is also increasing day by day. There is various kind of virus also various kind of mechanism to catch that virus which needs proper analysis.In this paper, there is a small survey of various kind of virus detection methods along with their consequences it does to the system.That will help to understand the merits and demerits of each virus after the survey.At the end, there is a conclusion and some information on what can be done to keep away from the virus in a large virtual world.

**Keywords :** Virus, Virus Detection, Signature-Based Virus Detection, Anomaly-Based Detection, Trojan

## 1. Details about Computer Virus

The Computer virus is a program which has the ability to replicate itself without anyone intervention and after that, the replicate program can replicate further,the same process goes on and on[2].As a result, the harmful code is a program which refers to something which function against the specification mentioned[3].There are many kinds of malicious code or programs which are designed to do some illegal or unauthorized functions which are really harmful to the system.There are many kinds of malicious software which are typically known as worms,trojan,malware etc a kind of virus.A computer virus contains three kinds of subroutines.Just like a normal virus causes the disease to our body similarly computer viruses are coded to propagate into the system without leaving the sign of the virus into the system.The virus affects the system by attaching with the other system programs like some application software.So sometimes when computer boots it enters into the system as it also affects the hard drive or boot media.Those are really deadly kind fo virus.The most serious effect it does when it controls some part of application like the browser,changes its settings,changing the system date,which sometimes difficult for a user to track the problem,sometimes virus delete a large amount of data also,in worst case modifying or crashing the whole system.There are many kinds of viruses.Viruses work like parasites which infect the systems.These programs are in the form of .exe file or .com file that controls another program.When someone clicks the .exe file in the computer ,the virus affects the system sometimes crashes the whole system which needs to be formatted again.

### 1.1 Boot sector virus

There are many formats of boot sector viruses are available.They are in major number as compared to all kind of computer viruses.Most risky computer virus till now.One of the popular boot sector virus is Michelangelo.They are difficult to detect.This kind of virus doesn't affect the normal performance of the computer always but silently it affects the removable media like floppy disks.The virus controls the system when the bootable media loads, as a result, the virus control the system before the operating system loads.it

attacks the RAM which attacks the hard disk that leads to restart of the system.

### 1.2 Trojan Horses

Just like another software program, it is a dangerous code,which tries to enter the system from backdoor without the knowledge of the normal user.After the certain period of time, it displays an error to the user,normal data of the disk can't be accessed,also sometimes the antivirus also can't detect the Trojan horse,so at that time reformating is really mandatory.Many great people said that Trojans are not the same kind of viruses as the damage caused by Trojan Horses are really very fast as compared to another kind of viruses [4].Examples are Back Office,Netbus,Nuker etc.

### 1.2 Stealth Viruses

Perhaps we have heard the name of Stealth aircraft which are specialized in hiding from radar,similarly stealth viruses are so strong that they can't be easily detected by radar or any other anti-virus programs.Though they are present in any part of the system or may be in boot media but any kind of scanner unable to detect the virus,it is what makes them so strong.It remains in the computer memory which is continuously monitoring the system.When some user opens a file in the system the virus infects the file,after that the virus automatically removes the infection from the system which makes them untraceable.They are not easily detected in boot sector as they go on changing the position of the boot sector,as a result, the computer will boot normally but slowly it leads to the very bad performance of the computer,also deletes some data,which leads to slowly killing off the system.

### 1.3 Adware

This kind of program effects the system when some clicks advertisement in the computer.The virus is injected in the advertisement,which will infect the system when someone clicks the add.As a result, it enters into the system along with that some malware and other harmful programs are there which can easily get control of the system with the help of this adware [5].Example : Adblaster, DeskAd, Clickbank

### 1.4 Metamorphic Virus

This kind of virus attacks in a network which is not easily to be track also.They change the code as well as the structure of them,which leads to a creation of a new virus which actually effects but nobody can trace the exact virus as their signatures changed,unable to match it technically[6] [7].Again after some time, it comes back to its original structure then again modify the internal structure takes another form so that a new virus again formed[2].

## 2. Other Kind of Virus

Many another kind of viruses or malware are there like Botnet,Logic Bomb,Rabbits,Scareware.Many different techniques are there to catch the virus,there are lots of antivirus programs which are available.The most popular security programs use potential scanning as well as it needs to be daily updated to work properly.After the proper scanning of the system, the virus is identified and terminated by the various tools which are installed in the system.Better the cost better is the service of the antivirus.

## 3. The threats of Viruses in the Operating Systems

There are certain loopholes in any operating system.Any virus just uses the loopholes of the system and gain access to the system software as well as application software of the system,which spreads continuously until it collapses the whole system.But still operating systems like UNIX have not so easily accessed by the virus ,inability to access the roots,but in Microsoft windows its is prone to many kinds of virus.in LINUX there are many fast updates which make it completely inaccessible for the virus.Some Linux versions keep the document in an undocumented way,some examples of those versions are Samba or NFS servers.Sometimes Linux servers are also accessed by malicious code where its script are attacked my malware so that any guest login can access them.

## 4. Virus detection methods

There is some virus detection method and there working is as follows:

### 4.1 Signature-based Virus Detection

This is the most common method deployed in all latest kind of anti-virus for identifying the virus.In the antivirus program, the signature of the known virus calculated from the data of virus file and those signatures are all stored in the database of the antivirus program.[8]When the program scans for the viruses it calculates the signature present in the system as per the data of the file and it compares with the signature it has already present in the database.If the signatures match as compared with the database,then the antivirus program declare that file as infected and it deletes the file.The accuracy of this kind of software depends on the database update,how frequently the database is updated[10].But every day the virus creators are creating new strategies to change the code so that the antivirus software don't detect the virus, the virus remains to hide,Sometimes after infecting a file,the virus changed its forms by mutating itself,so sometimes it is untraceable to detect the virus easily.Each time the mutation performs the same kind fo function as the parent.This kind of virus is also known as self-mutating virus[9].In this kind of techniques, the chances of false alarm are very less.Just the requirement is always the updated database of all signatures of virus.The perfect result depends on the signature present in the database.It generally doesn't detect a new virus as the signature of that virus is not present in the database.Here the opcode pattern is followed for the signature of the input file.

### 4.2 Anomaly based virus detection

In this kind of detection techniques, it processes the host machine for any kind of suspicious activity.If in case any kind of suspicious activity is detected the system raises an alarm which informs the possible chances of virus or malwares[10].Sometimes the chances of false alarm are more but it is good for use because chances of catching new virus are also more.Here the raising alarm is not so dangerous as allowing a new virus to enter into the system.Sometimes any hacker group can enter into the system which controls the alarm and makes the abnormal behavior as normal[11].As a result, the system fails to detect the abnormal behavior in such case[10].The meaning of anomaly is something which is not normal.New kind of malware or virus is detected without even have to worry about the database is updated.Some small maintenance is sufficient to monitor the network activity,the more the system is in use the more chances of catching the virus.Sometimes the network is not safe as the system builds its profile.If any kind of virus activity looks normal then it will not give any alarm.So small checking such as routing checking or even after checking email can also lead to signal alarm.Which is one of the bad features of this kind of detection techniques.

### 4.3 Code Emulation

This is the most effective virus detection technique.A virtual machine is there to simulate CPU and memory activities for the code activity. It uses a debugger interface to trace the code along with the processor ,this type is not safe enough as the code jump out of the environment during analysis.This kind of technique is more powerful in dealing with the polymorphic virus as well as encrypted virus[12].

### 4.4 Virus-specific Detection

It happens sometimes the particular algorithm can't detect the virus. For such cases, a virus-specific detection algorithm is developed to implement the detection procedure.This kind of technique is not the common method but it is used in particular cases to catch certain kind of virus.This kind of detection is called algorithm detection method. But because it can me misleading[13],generally virus-specific detection is used instead of algorithm scanning.It has many drawbacks also due to its stability as well as platform related problems also portability.For this virus scanning languages have been developed in simple form,seeking and reading operations in a lucid form.

### 4.5 Filtering

This method is used to increase the performance of anti-virus program regarding the scanning speed.This is used in certain virus detection method because those are very time-consuming and also complexity in performance.as the virus infects the file ,based on the signature it can be classified as .com and .exe files,script ,boot sector and there are much more. Any executable file infects .exe and .com. Only the signature is used to decrease the scanning time.

**5. Solutions for Virus Problems**

Apart from using anti-virus software, there are other procedures which can help protect against viruses some of which include:-

- Running scheduled scan, updated virus scan software on all computers within the organization at least once a week.
- Keeping software patches updated with some updates can be downloaded from websites.
- Updating the antivirus frequently,if possible daily basis.
- Use licensed version of any software, don't use cracked software or tools or patches,it may include some kind of virus or malware.
- Don't give administrative privileges to anyone,as it may increase the chance of getting infected.
- Don't use free antivirus ,as it doesn't support the full functionality of the software,it needs to be paid version.
- Keep sufficient backup of data ,if a system needs to be restored due to certain infection in the system.
- If any harmful virus already entered into the system,then formatting the system is the best possible option.

**6. Comparison Study**

| | **Strength** | **Limitation** | **Cost** | **Accuracy** |
|---|---|---|---|---|
| **Anomaly Based Detection** | Detects new virus | Not detects all kind of malware | Very costly | Good result |
| **Virus-specific Detection** | helpful after implementation of proper algorithm | Not suitable for multiple viruses | Practically complex to implement | At some cases helpful |
| **Code Emulation** | Best for encrypted virus | Very complex design | Very costly | Good result |
| **Filtering** | Increases the scanning speed | Complex design | No such proof | good |
| **Signature based virus detection** | Good result on updated database | Can't detect if database not updated | Affordable cost | Detect most of malwares |

In various virus detection techniques, everyone has certain advantages as well as disadvantages. For signature-based detection it is a helpful tool because it matches the signature from the database. It is very simple as well as effective for the best result. It has a limitation that it can't detect new virus if the database is not updated. Whereas Anomaly based detection is beneficial for any abnormal function in the system, which is beneficial for detecting new kind of viruses without any issue of database updated or not. Sometimes it can't deletes the non affected files also. In code emulation technique it is powerful for polymorphic or encrypted virus in the system, there is no other best encrypted virus detection technique than this.Whereas the complexity is more in this kind of techniques. Code emulation technique is very costly to implement. Virus detection method is used when particular algorithm is required to detect some kind of virus. There are many techniques which are not good for unknown viruses[14].Also the time taken to scan the system is more ,as a result sometimes the virus are not detected, also many known virus are detected easily not for all kind of viruses. In anomaly base technique it is really difficult to detect virus which behaves normally[14].

## I. CONCLUSION

Although antivirus programs are daily updated still it virus creators are daily updating as well as modifying the code which makes the system more vulnerable to attacks.Only after a virus is launched on the system then only anti-virus are launched in the market with latest methodologies,that makes us think that still there is still large core area development is required in the virus detection techniques.Now large network needs to be monitored for the attacks by malware,virus,Trojan

etc.So that the virus needs to be deleted first before it removes any valuable data of any organization.Also in latest technologies the time complexity has to be reduced along with the quality of hardware needs to be considered before implementing good quality of software,that automatically reduces the chance of getting infected by the malicious thing.Companies need to invest more focus on the research and development area so that good tech savvy are required in the current scenario.Common people needs to be trained from the anti-virus companies for the basic security level of their systems.It can reduce the chances of getting infected.

## II. ACKNOWLEDGMENTS

Many Many thanks to all the references names given below,because of there great help,this journal creation is possible.They are great guides for the preparation of this journal,there journals are in great help for research.

## III. REFERENCES

[1]. Dr. Prof. Milind. J. Joshi , Mr. Bhaskar V. Patil ,Shivaji University Kolhapur, Kolhapur M.S.], INDIA,Computer Virus: Their Problems & Major attacks in Real Life,ISSN: 2249-2615

[2]. Dr. Solomon's Virus Encyclopedia, 1995, ISBN 1897661002

[3]. Dr. Klaus Brunnstein 1999, from Antivirus to Antimalware Software and Beyond http://csrc.nist.gov/nissc/1999/proceeding/papers/p12.pdf

[4]. H. Shravan Kumar, "Seminar Report on Study of Viruses and Worms",Indian Institute of Technology Bombay, 2005.

[5]. K. Mathur, S. Hiranwal, "A Survey on Techniques in Detection and Analyzing Malware Executables", International Journal of Advanced Research in Computer Science and Software Engineering, ISSN: 2277 128X, Vol. 3, Issue 4, April 2013

[6]. Hossein Bidgoli, Handbook of Information Security, Volume 3,1st Edition, John Wiley & Sons, ISBN-10: 0471648337, ISBN-13: 978-0471648338, December, 2005

[7]. S. Venkatachalam, M. Stamp, "Detecting Undetectable Metamorphic Viruses", Proceedings of the 2011 International Conference on Security & Management (SAM 2011), pp. 340-345, 2011,ISBN-10: 1-60132-196-1.

[8]. D.RAKESH, L. PADMALATHA,PATTERN MATCHING ALGORITHM USING FILTER ENGINE AND EXACTMATCHING ENGINE, INTERNATIONAL JOURNAL OF ENGINEERING RESEARCH & TECHNOLOGY (IJERT)VOL. 1 ISSUE 7, SEPTEMBER – 2012

[9]. Min Feng Rajiv Gupta, Detecting Virus Mutations Via Dynamic Matching, CSE Dept., University of California

[10]. Ankush R Kakad, Siddharth G Kamble, Shrinivas S Bhuvad, Vinayak N Malavade , Study and Comparison of Virus Detection Techniques , Volume 4, Issue 3, March 2014 , ISSN: 2277 128X

[11]. Jan Hruska. Computer Viruses and Anti-VirusWarfare. Ellis Horwood, Chichester, England,

[12]. Wing Wong, ANALYSIS AND DETECTION OF METAMORPHICCOMPUTER VIRUSES, A Writing Project Presented toThe Faculty of the Department of ComputerScienceSan Jose State University.

[13]. Szor, P., The Art of Computer Virus Research and Defense, Addison-Wesley Professional, 2005.

[14]. ESSAM AL DAOUD1, IQBAL H. JEBRIL2AND BELALZAQAIBEH, COMPUTER VIRUS STRATEGIES AND DETECTIONMETHODSESSAM ,INT. J. OPEN PROBLEMS COMPT. MATH., VOL. 1, NO. 2, SEPTEMBER 2008.