ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

A Survey: Analysis of Virus and Malware Detection

A.Anupriya[1], V.Nithya[2], S.Ponmalar[3]

III B.Sc Computer Science, Department of Computer Science, Sri G.V.G.Visalakshi College for Women, Udumalpet, India.[1, 2]

Assistant Professor, Department of Computer Science Sri G.V.G.Visalakshi College for Women, Udumalpet, India.[3]

ABSTRACT: In latest years the detection of computer viruses has become general place. Computer viruses stay behind a significant threat to computer networks. Through the study of the model, bug-free and common stability points are calculated. To show our abstract analysis, some numerical simulations are also included. The results provide a theoretical basis to control the widen of computer virus. The usual antivirus approach consists of waiting for a number of computers to be infected, detecting the virus, scheming a solution, and delivering and deploying the clarification, in such situation, it is very hard to prevent every machine from being compromised by virus. In this paper we discussed analysis of virus algorithm.

KEYWORDS: Virus, Virus Detection, Virus Analysis, Virus Algorithm.

I. Introduction

A computer virus is a type of malevolent software program. Infected computer programs can include, as well, data files, or the "boot" sector of the hard drive. The computer virus is one common information security threat. The huge majority of viruses target systems running Microsoft Windows. Computer viruses currently cause billions of dollars' worth of economic spoil each year, due to causing system failure, wasting computer resources, corrupting data, increasing maintenance costs, etc. In response, free, open-source antivirus tools have been developed, and an industry of antivirus software has cropped up, selling or freely distributing virus guard to users of various operating systems. Even though no currently antivirus software was capable to uncover all computer viruses (especially new ones), computer security researchers are actively incisive for new ways to enable antivirus solutions to more effectively detect emerging viruses, before they have already become broadly spread. The term "virus" is also commonly, but incorrectly, used to refer to other types of malware [1]. "Malware" encompasses computer viruses along with many other forms of malevolent software, such as computer worms, ransom ware, spyware, adware, Trojan horses, key loggers, root kits, boot kits, malicious Browser Helper Object (BHOs) and other malicious software. The majority of active malware threats are actually trojan horse programs or computer worms rather than computer viruses.

II. Virus History

The word computer virus, coined by Fred Cohen in 1985. Computer viruses were first termed simple 'bugs' when systems were found to be crashing or incurred various technical problems. In the early 1940s, this wasn't a trouble that could increase to other computers so without problems since networking and linking computers through a large-scale computer communication system was not established. As computer networks evolved and established into the personal and business sector during the early 1990s, more people realized the need for the best antivirus software and shielding networked computers from potential threats[2]

A virus is, in fact, the earliest known malware invented.

The following is a history of some of the most famous viruses and malware ever:

1949 – 1966 - Self-Reproducing Automata

DOI: 10.15680/IJIRCCE.2018.0603122

1959	- Core Wars
1971	- The Creeper
1974	- Wabbit (Rabbit)
1974 – 1975	- ANIMAL
1981	- Elk Cloner
1983	- Virus
1986	- Brain
1987	- Lehigh, Cascade,Jerusalem Virus
1988	- The Morris Worm
1990	- Chameleon
1995	- Concept
1996	- Laroux, Baza
1998	- CIH Virus
1999	- Happy99
2000	- ILOVEYOU
2001	- Anna Kournikova
2002	- LFM-926
2004	- MyDoom
2005	- Samy XXA.
2006	- OSX/Leap-A
2007	- Storm Worm, Zeus
2008	- Koobface
2010	- Kenzero
2013	- Cryptolocker
2014	- Backoff
2014	- Regin
2015	- BASHLITE
2016	-Ransomware Locky, Banker, Trojan,
2017	-WannaCry ransomware

III. Features and Types of Virus

Again mention that virus is a program. Therefore each virus has different code and algorithm. These virus algorithms can be differentiated according to their features as each algorithm is designed for some specific task.

Features of operating algorithms:

- Ability of virus to cover traces
- Use of Self encryption
- Polymorphic capability
- Metamorphic code Algorithm
- Terminate and Stay Resident capability
- Use of non-standard techniques

ISSN(Online): 2320-9801
ISSN (Print) : 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Website: www.ijircce.com

Vol. 6, Issue 3, March 2018

Types of Viruses:

Most Common Types of Viruses and Other Malicious Programs

- Resident Viruses
- Multipartite Viruses
- Direct Action Viruses
- Overwrite Viruses
- Boot Virus
- Macro Virus
- Directory Virus
- Polymorphic Virus
- File Infectors
- Encrypted Viruses
- Companion Viruses
- Network Virus
- Nonresident Viruses
- Stealth Viruses
- Sparse Infectors
- Spacefiller (Cavity) Viruses
- FAT Virus
- Worms
- Trojans or Trojan Horses
- Logic Bombs
-

Other Kind of Virus:

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

Popular methods of virus detection

One of the most essential functions of any anti-virus program is to detect the presence of any virus in a computer system. Once a virus is detected, the antivirus program usually informs the user about the detection of the virus. Since the virus often writes its code into the program at some different locations the anti-virus tries to eliminate the virus codes and restore the original program[3].

An anti-virus program uses various methods for detecting viruses. As the characteristics of different viruses are different their detection methods are also different. All types of viruses cannot be detected by any single method. The popular methods used by the anti-virus programs for detecting viruses are as follows:

- Signature scanning
- Integrity checking
- Heuristic scanning
- Emulations
- Activity monitoring

DOI: 10.15680/IJIRCCE.2018.0603122

IV. Comparioson of Virus Detection Methods

We here evaluate three methods of virus detection that is Signature based virus detection, Anomaly Based Detection, Code Emulation on the basis of parameter. Strength of Signature based virus detection is better because it depend on comparing the signature. Anomaly Based Detection is best for the detection of new viruses, while Code emulation is best for detection of encrypted viruses. Limitation of Signature based virus detection that it cannot detect new malware when database is not updated. Limitation of Anomaly Based Detection technique is that some time it remove unaffected file also.

Limitation of Code Emulation is that this method is very complex to implement. Cost of Signature based virus detection

is low it require only database to store the signature of viruses. Anomaly Based Detection method require monitoring the activity of process each time which is more costly and time consuming. Code Emulation is costly method it require execution of virtual machine to detect virus. Accuracy of Signature based virus detection is more if database is updated. In Anomaly Based Detection is not always potential to get accurate result by only monitoring process activity some time it can give wrong result. Accuracy is more in Code Emulation method because it implements virtual machine to detect the viruses [1].

Avoid viruses and spyware

1: Install quality antivirus
2: Install real-time anti-spyware protection
3: Keep anti-malware applications current
4: Perform daily scans
5: Disable auto run
6: Disable image previews in Outlook
7: Don't click on email links or attachments
8: Surf smart
9: Use a hardware-based firewall
10: Deploy DNS protection

V. 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. It can reduce the chances of getting infected.The simplest and most economical for detecting the majority of current viruses is signature scanning. While signature scanning may not be able to detect all possible viruses, but it is still simple and cheap enough to be easily available and useful to the public at large and it has the least impact on existing code and hardware. Present world is the era of information technology which has made the sharing of information a click away. But this technology has generated adverse effects also one of which is virus i.e. with the generation of new technologies new viruses are also coming up every day. There are new anti-virus programs and techniques developed too. It is good to be aware of viruses and other malware and it is cheaper to protect your environment from them using latest antivirus software rather than being sorry. If your system starts behaving differently it means your system has been infected. There are many viruses which behave differently from general concepts regarding viruses e.g. Trojan horse virus and Macros.

A Trojan horse is not a virus because it doesn't reproduce. The Trojan horses are usually masked so that they look interesting. These viruses that pinch passwords and format hard disks.

Macro viruses spread from applications which use macros. These viruses' spreads fast through internet because people share so much data, email documents and use the Internet to get documents. The mission of viruses is to move from one program to other and this can happen via floppy disks, Internet FTP sites, newsgroups and via email attachments. Viruses are mostly written for PC-computers and DOS environments. Today every user has to deal with viruses. For good security appropriate passwords, proper access controls and careful design are still needed. These protection measures act as similar as the body's skin and innate immune system, which are responsible for preventing most infections. This paper has focused on the human immune system's adaptive responses, because these are the types of mechanisms current computer systems do not have. By removing these shortcomings, it is possible to make computer systems much more secure.

ACKNOWLEDGMENT

The authors express their sincere thanks to **Ms.S.Ponmalar M.Sc., M.Phil (Computer Science)., Assistant Professor,** Department of Computer Science, Sri G.V.G.Visalakshi College for Women, Udumalpet, for her constant help, keen interest, valuable guidance and advice throughout the period of study and enabling me to carry out this work in our favorite Computer technology area.

We would like to express our sincere thanks to our HOD madam and all the **Staff Members** of **Department of Computer Science** who were responsible for the good finish of this dissertation.

we wishes to express our deep indebtedness to our **Loving Parents, Sister, Brother,** for enabling her to do this study and constantly supporting. Last but not the least she extends her thanks to her **Friends** and **All Wishers** for being the motivating force behind this article and the providing normal support and encouragement in carrying out the work.

REFERENCES

[1] Soumen Chakraborty ," A Comparison study of Computer Virus and Detection Techniques ",International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT | Volume 2 | Issue 1 | ISSN : 2456-3307

[2] Soumen Chakraborty ,"A Comparison study of Computer Virus and Detection Techniques" International Journal of Scientific Research in Computer Science, Engineering and Information Technology © 2017 IJSRCSEIT | Volume 2 | Issue 1 | ISSN : 2456-3307

[3] Ankush R Kakad, Siddharth G Kamble, Shrinivas S Bhuvad, Vinayak N Malavade," Study and Comparison of Virus Detection Techniques", International Journal of Advanced Research in Computer Science and Software Engineering Volume 4| Issue 3| March 2014 | ISSN: 2277 128X

″A Comparative Study for Performance Measurement of Selected Security Tools ″. Mr. B.V. Patil, Dr. Prof. M.J. Joshi, Mr.H.N. Renushe. International journal of scientific & Engineering Research, Volume 1, Issue 1, October-2010.

[4] ″A Proposed antiviruses strategy for a Complex environment with a huge Number of viruses attacks″. Mohammad Alaa Hussain Al-Hamami, Volume 2 No.6, JUNE 2011 ISSN 2079-8407 Journal of Emerging Trends in Computing and Information Sciences.

[5] ″A Comparative Study of Virus Detection Techniques″. Sulaiman Al Amro, Alkhalifah, International Journal of computer, Electrical, Automation, Control and Information Engineering Vol:9, No:6, 2015.

[6] ″Study and Comparison of Virus Detection Techniques″. Ankush R Kakad, Siddharth G Kamble, Shrinivas S Bhuvad, Vinayak N Malavade. International Journal of Advanced Research in Computer Science and Software Engineering. Volume 4, Issue 3, March 2014 ISSN:2277 128X.

[7] ″Comparative analysis of feature extraction methods of malware detection″. Smita Ranveer, Swapnaja Hiray. International Journal of Computer Applications. (0975 8887). Volume 120 – No.5, June 2015.

[8] ″Malware Analysis and Classification: A Survey″ Ekta Gandotra, Divya Bansal, Sanjeev Sofat.Journal of Information Security, 2014, 5, 56-64 Published Online April 2014 in SciRes.

[9] ″Comparative Study and a Survey on Malware Analysis Approaches for Android Devices″ Minakshi Ramteke, Prof. Praveen Sen and Suchit Sapate. International Journal of Advanced Research in Computer Science and Software Engineering Research Paper

[10] ″Comparison of Anti-Virus Programs using Fuzzy Logic″Vaclav Bezdek Thomas Bata University, Zlín, Czech Republic. URL:http://www.avcomparatives.org/comparativesreviews/summ aryreports/137-summary-report-december- 2011

[11] ″Selection of Next Generation Anti-Virus against Virus Attacks in Networks Using AHP″Sounak Paul,Bimal Kumar Mishra. International Journal of Computer Network and Information Security(IJCNIS) ISSN: 2074-9090 (Print), ISSN: 2074-9104 (Online). IJCNIS Vol. 5, No. 2, February 2013.

[12] ″Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey″Babak Bashari Rad1, Maslin Masrom2 and Suhaimi Ibrahim3. IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1, January 2011 ISSN (Online): 1694-081