ISSN:2321-0613

Computer Viruses and Detection : A review

Prof. Deepali Maste[1] Prof. Mahendra Patil[2] Prof. Rajesh Gaikwad[3]
[1,2,3]Assistant Professor
[1,2,3]Department of Computer Engineering
[1,2,3]Atharva College of Engineering, Mumbai University,Mumbai, India

Abstract— This paper reviews computer virus and few detection techniques. Computer viruses can wreak havoc to the operations of the computer. A computer virus is a type of malware that is intentionally written to gain entry into your computer, without your knowledge or permission. There are various types of computer viruses, classified in terms of techniques, origin, and the types of files affected, damage, OS or Platform attacked, as well as the places they hide. Many techniques like Signature based virus detection, Anomaly based virus detection and Emulation based detection,Neural network, SICS model studied here.

Key words: Computer Virus, Neural network, virus types, virus detection

I. INTRODUCTION

There are varying different types of computer viruses and their effects also vary widely. While some simply replicate themselves, others adversely affect the programs and consequently, the system's performance. The most common types of viruses seen in 2014 – 2015 that have a high impact on users are Browser Highjack viruses. Generally this type of infection is not really a virus but something called PUP or Potentially unwanted software. Computer viruses can wreak havoc to the operations of the computer. A computer virus is a type of malware that is intentionally written to gain entry into your computer, without your knowledge or permission. It has the capacity to modify or replicate itself, in which case it will continue spreading. In most cases these browser highjacks change the users' home page and search settings in the web browser and often make it extremely hard to remove and restore the default settings. These kinds of browser highjacks get installed from bundled software that may include free programs such as computer games or wall papers.

Different types of computer viruses would reach you through the typical web activities like, Opening email attachments from fake accounts, Clicking inappropriate internet advertisements without understanding fully, Installing/ downloading the free games, toolbars or system utilities, visiting an infected web page and setting up of software without license agreements etc..

There are various types of computer viruses, classified in terms of techniques, origin, and the types of files affected, damage, OS or Platform attacked, as well as the places they hide.

Resident viruses are permanent viruses dwelling in RAM memoryTheir effects include corrupting programs and files that are closed, opened, renamed or copied.Overwrite viruses delete information that is in the infected files. Direct action viruse replicates itself, and then acts when executed; the virus infects files located in the folders or computer directory. File infectors virus infects executable files or programs. On running the programs, the virus would be activated, then be able to carry out its damaging effects. Boot viruses infect the hard disk's or floppy drive's boot sector. This would make the computer unable to boot. Directory viruses alters the paths indicating a file's location, when the infected program is executed, you will be running the program unknowingly, since the virus has moved the original program and file to another location. Macro virus affects files created using particular programs or applications containing macros.

II. LITERATURE SURVEY

Different types of virus detection techniques are invented to overcome the problem of virus anomaly. But still none of the system assures us complete virus free environment plethora of negative magazine articles and books have catalyzed a new kind of hypochondria among computer users: an unreasonable fear of computer viruses. This hypochondrium is possible because a) computers are very complex machines which will often behave in ways which are not obvious to the average user, and b) computer viruses are still extremely rare. Thus, most computer users have never experienced a computer virus attack [1].

Viruses require a host, and their goal is to infect other files so that the virus can "live" longer. Some viruses perform destructive actions although this is not necessarily the case. Many viruses attempt to hide from being discovered. All viruses make copies of themselves, infecting boot sectors, programs, or "data files" as the opportunity arises [2].

Shivani Shah proposed in her paper [3] utilization of neural networks to create a system which is self-learning. The inputs considered for the neural network training are the various fields of Portable Executable structure (PE structure). Various PE header attributes are collected and provided as input to train the neural network. In her paper, various feature selection algorithms have been studied and Fisher Score was found to be the most appropriate one. Using this, the most relevant features PE Structure were found out which can be given as inputs to the neural network[3].

In Virus Detection Systems Sujandharan Venkatachalam [4] proposes three types of detection Signature based virus detection, Anomaly based virus detection and Emulation based detection. Signature based detection systems scan the files for specific signatures that are present in them. The pattern of instructions present in a virus code is identified as the signature of the virus file. This will raise an alarm for virus if the signature of a virus is detected in any of the files scanned. Anomaly based detection systems monitor the processes on a host machine for any abnormal activity. In this detection technique, the system uses the collected heuristics to categorize an activity as normal or malicious. Even though chances of false alarm are relatively higher in this method, it is more reliable because it is also capable of detecting new viruses. The emulation based detection is an effective method where a virus is executed in a virtual environment by emulating the instructions in the virus code. This type of detection is used to detect polymorphic, as well as metamorphic, viruses [4].

Tesauro, G.J. has developed a neural network for generic detection of a particular class of computer viruses- the so called boot sector viruses that infect the boot sector of a floppy disk or a hard drive. This is an important and relatively tractable sub problem of generic virus detection. Only about 5% of all known viruses are boot sector viruses, yet they account for nearly 90% of all virus incidents. We have successfully deployed our neural network as a commercial product, distributing it to millions of PC users worldwide as part of the IBM AntiVirus software package [5].

The recently proposed SICS model by Xu, Xun[6] takes into account the dissemination of countermeasures as well as the propagation of viruses; as thus, it offers a new approach to the evaluation of effectiveness of countermeasure strategies. However, the linear assumption of the infection rate in the SICS model fits well with the real situation only when the number of infected node is very small. To better understand the virus-countermeasure mixed behavior, in his paper the SICS model is modified by introducing a nonlinear infection rate [6].

III. Conclusion

Computer Viruses are the well-known computer attackers and they can drastically slow down its operation. The increasing importance of networked control systems makes them inviting targets for cyber-attacks. Moreover, due to the easy installing nature of malicious programs, computer users suffer with the data loss and system disruption. So it is essential to take some security measures by installing effective anti-virus software to ensure your computer protection. Study of few virus detection techniques explores different ways in which this anomaly can be detected. In the reviewed literature neural network seem the most promising way of assurance of virus detection as in compared with other techniques it can be one of the preventive way to solve virus problems. Though more study and research is required in this domain.

References

[1] Mark A. Ludwig ,The Little Black Book of Computer Viruses Volume One: The Basic Technology By American Eagle Publications, Inc. Post Office Box 1507 Show Low, Arizona 85901 - 1996 –

[2] Snorre Fagerland, Sylvia Moon, Kenneth Walls, Carl Bretteville, Norman Book on Computer VirusesCopyright © 1990-2003 Norman ASA.

[3] Shivani Shah, Himali Jani, Sathvik Shetty, Kiran Bhowmick Virus Detection using Artificial Neural Applications (0975 – 8887) Volume 84 – No 5, December 2013

[4] Sujandharan Venkatachalam, Detecting undetectable computer viruses, Report Presented to The Faculty of the Department of Computer Science San Jose State University In May 2010

[5] Tesauro, G.J. IBM Thomas J. Watson Res. Center, Yorktown Heights, NY, USA Kephart, J.O. ; Sorkin, G.B.,Neural networks for computer virus recognition, Browse Journals & Magazines IEEE Expert . Volume: 11 Issue:4 , Aug 1996

[6] Xu Xun,Yang,Xiaofan,Li Chuandong, "Towards the understanding of the mixed behavior of electronic viruses and countermeasures, ICICIP 2015 Sixth International conference at Wuhan China, ISBN 978-1-4799-175-0 26-28 Nov 2015