ISSN No. 0976-5697

Volume 2, No. 5, Sept-Oct 2011

International Journal of Advanced Research in Computer Science

REVIEW ARTICLE

Available Online at www.ijarcs.info

Computer Viruses Become Dangerous to Technical and Operational Structure of Computer

Shashi Shekhar Ranga
Research Scholar
JJT University,
Chudela, Jhunjhanu, India
ranga.ssr@gmail.com

Abstract: This paper describe the computer viruses as in technical i.e. hardware and operating i.e. software Functions with their history, and of the various ways of spreading computer viruses. Computer virus is code that recursively replicates a possibly developed copy of itself. Viruses infect a host file or system area, or they simply modify a reference to such objects to take control and then multiply again to form new generations. Latter we demonstrate various sides of the virus in other words some dark side i.e. about its history and their affect on hardware and software.

Keywords: virus, computer, software, hardware

I. INTRODUCTION

The term computer virus is derived from Latin which means poison. From last few years virus become very highlighted as destructor. One of the biggest fears among new computer users is being infected by a computer viruses or programs which are designed by them to destroy their personal data. Viruses are being defined as malicious software programs that have been designed by other computer users to cause destruction and havoc on a computer and spread themselves to other computers where they can repeat the process. Computers are designed to execute instructions one after another; On the other hand, the instructions executed can be damaging and malicious in nature. When that happens by accident, we call the code involved software bug perhaps the most common cause of unexpected program behavior. If the source of the instructions was an individual who intended that the abnormal behavior occur, then we consider this malicious coding; authorities have sometimes referred to this code as malware and vandal ware. These names relate to the generally effect of such software. In recent years, occurrences of malware have been described almost uniformly by the media as computer viruses. Viruses are widespread, but they are not responsible for many of the problems attributed to them.

A computer virus is a segment of machine code (typically 200-4000 bytes) that will copy itself (or a modified version of itself) into one or more larger "host" programs when it is activated. When these infected programs are run, the viral code is executed and the virus spreads further. Computer viruses cannot spread by infecting pure data; pure data files are not executed.

II. HISTORY

The first use of the term virus to refer to unwanted computer code was by the science fiction author David Gerrold. He wrote a series of short stories about a fictional G.O.D. machine (super computer) in the early 1970s that were later merged into a novel in 1972.The description of virus in that book does not fit the currently-accepted, popular definition of computer virus "a program that alters other programs to include a copy of itself".

Fred Cohen formally defined the term computer virus in 1983. [2]. Dr. Cohen's Ph.D. thesis and later research were devoted to computer viruses. Actual computer viruses were being written by individuals before Cohen, although not named such, as early as 1980 on Apple II computers. [9] Although Cohen (and others, including Len Adelman [1]) has attempted formal definitions of computer virus, not have gained widespread acceptance. This is a result of the difficulty in defining precisely the characteristics of what a virus is and is not. Cohen's formal definition includes any programs capable of self-reproduction. So, by his definition, programs such as compilers and editors would be classed as "viruses." "He defines a virus as a piece of code with two characteristics:

a. At least a partially automated capability to reproduce.
b. A method of transfer which is dependent on its ability to attach itself to other computer entities (programs, disk sectors, data files, etc.) that moves between these systems."[15, p. 145].

In particular, they have flourished in the weaker security environment of the personal computer.

III. VARIOUS WAYS OF VIRUSES

The systems contained no security facilities beyond an optional key switch, and there was a minimal amount of security-related software available to safeguard data. Today, however, personal computers are being used for tasks far different from those originally visualized, including man aging company databases and participating in networks of computer systems. Unfortunately, their hardware and operating systems are still based on the assumption of single trusted user access, and this allows computer viruses to spread and flourish on those machines. The population of users of PCs further adds to the problem, as many are unsophisticated and unaware of the potential problems

involved with negligent security and uncontrolled sharing of media.

Viruses are represented by patterns of computer instructions that exist over time on many computer systems. Viruses are not associated with the physical hardware, but with the instructions executed (sometimes) by that hardware. The patterns of the viruses are a temporary set of electrical and magnetic field changes in the memory or storage of computer systems.

IV. SELF-REPRODUCTIION OF VIRUSES

One of the primary characteristics of computer viruses is their ability to reproduce themselves (or an altered version of themselves). it is possibly more interesting to examine this aspect in light of the agent of reproduction. The virus code is not itself the agent the computer is. It is questionable if this can be considered sufficient for purposes of classification as artificial life. To do so would imply that (for instance) the blueprints for a Xerox machine are capable of self-reproduction: when outside agents follow the instructions therein, it is possible to produce a new machine that can then be used to make a copy of them.

V. FUNCTIONAL PENETRATION WITH THE VIRUSES ENVIRONMENT

Viruses perform examinations of their host environments as part of their activities. They alter interrupts, examine memory and disk architectures, and alter addresses to hide themselves and spread to other hosts. They very obviously alter their environment to support their existence. Many viruses accidentally alter their environment because of bugs or unforeseen interactions. The major portion of damage from all computer viruses is a result of these interactions.

VI. EFFECT OF VIRUSEES ON HARDWARE AND SOFTWARE

Few viruses are written with redundant code, and even so, the working code cannot be divided without disabling the virus. However, it is interesting to note that the virus can be reassembled later and regain its functional status. Computer viruses run on a variety of machines under different operating systems. Many of them are able to compromise anti-virus and copy protection mechanisms. They may adjust on-the-fly to conditions of insufficient storage, disk errors, and other exceptional events. Some are capable of running on most variants of popular personal computers under almost any software configuration stability and robustness seen in few commercial applications.

VII. OTHER BEHAVIOUR OF VIRUSES

Some viruses also show greedy behaviour. For e.g., the DenZuk virus will seek out and overwrite example of the Brain virus if both are present on the same system. Other viruses exhibit territorial behaviour marking their infected domain so that others of the same type will not enter and compete with the original infection. Some viruses also exhibit self-protective behaviour, including camouflage techniques. These changes have been in reaction to a supposed need to “enhance” the virus usually to make it more difficult to find.It might well be argued that more traditional living organisms may also undergo change from without.

A. Growth of Viruses:

Viruses certainly do show a form of growth, in the sense that there are more of them in a given environment over time. Some temporary viruses will infect every file on a system after only a few activations. The spread of viruses through commercial software and public bulletin boards is another indication of their wide spread replication. Although accurate numbers are difficult to derive, reports over the last few years indicate an approximate yearly doubling in the number of systems infected by computer viruses. Clearly, computer viruses are exhibiting significant growth.

VIII. CONCLUSION

The origin of most computers viruses are one of unethical practice. Viruses created for malicious purposes are obviously bad; viruses constructed as experiments and released into the public domain would likewise be unethical and poor science besides: experiments without controls, strong hypotheses, and the consent of the subjects. From the study of computer viruses: the critical realization that experimentation with systems in some ways (almost) alive can be hazardous. Computer viruses have caused millions of dollars of damage and untold aggravation.

Research into computer viruses may be of some scientific interest. By modeling behavior using computer viruses, we may be able to gain some insight into systems with more complex interactions. Research into competition among computer viruses and other software, including anti-viral techniques, is of practical interest as well as scientific interest. Modified versions of viruses such as Thimble by’s Live ware may also prove to be of ultimate value. The problem with research on computer viruses is their threat. True viruses are inherently unethical and dangerous. They operate without consent or knowledge, experience has shown that they cannot be recalled or controlled, and they may cause extensive losses over many years. Even viruses written to be benign cause significant damage because of unexpected interactions and bugs.

Additionally, their replication is generally under the close control or observation of their users. however. If we are to continue to research computer viruses, we need to find fail safe ways of doing so. This is a major research topic in itself. The danger of creating and accidentally releasing more sophisticated viruses is too great to risk, especially with our increasing reliance on computers in critical tasks. It would be especially dangerous to attract the untrained, the careless, and the uncaring to produce them.

IX. REFERENCES

[1]. Leonard Adleman. An abstract theory of computer viruses. In Lecture Notes in Computer Science, vol 403. Springer-Verlag, 1990.

[2]. Fred Cohen. Computer Viruses. PhD thesis, University of Southern California, 1985.

[3]. Frederick B. Cohen. A Short Course on Computer Viruses. ASP Press, Pittsburgh, PA, 1990.

[4]. Frederick B. Cohen. Friendly contagion: Harnessing the subtle power of computer viruses.The Sciences, pages 22–28, Sep/Oct 1991.

[5]. Peter J. Denning, editor. Computers Under Attack: Intruders, Worms and Viruses. ACM Press(Addison- Wesley), 1990.

[6]. Tom Duff. Experiences with viruses on Unix systems. Computing Systems, 2(2), Spring 1989.

[7]. Mark W. Eichin and Jon A. Rochlis. With microscope and tweezers: an analysis of the internet virus of november 1988. In Proceedings of the Symposium on Research in Security and Privacy, pages 326–343, Oakland, CA, May 1989. IEEE-CS.

[8]. J. Doyne Farmer and Alletta d'A. Belin. Artificial life: The coming evolution. In Proceedings in Celebration of Murray Gell-Man's 60th Birthday. Cambridge University Press, 1990. To appear.

[9]. David Ferbrache. A Pathology of Computer Viruses. Springer-Verlag, 1992.

[10]. Christopher V. Feudo. The Computer Virus Desk Reference. Business One Irwin, Homewood, IL, 1992.

[11]. Philip Fites, Peter Johnson, and Martin Kratz.The computer virus crisis. Van NostrandReinhold, 2nd edition, 1992.

[12]. David Gerrold. When Harlie Was One. Doubleday, Garden City, NY, 1972.

[13]. William Gibson. Neuromancer. Ace/The Berkeley Publishing Group, 1984.

[14]. Harold Joseph Highland, editor. Computer Virus Handbook. Elsevier Advanced Technology, 1990.

[15]. Brad Stubbs and Lance J. Hoffman. Mapping the virus battlefield. In Hoffman [15], chapter 12, pages 143–157.

[16]. Jan Hruska. Computer Viruses and Anti-Virus Warfare. Ellis Horwood, Chichester, England, 1990.