World Journal of Research and Review (WJRR)
ISSN: 2455-3956, Volume-14, Issue-5, May 2022 Pages 39-44

A Review Study on Computer Virus

Priya Bhargava, Rahul Choudhary, Ankesh Gupta

***Abstract*— As we all aware of the word computer virus. What we know is that it is a virus that affect computer system but we don't know how it works and how it affect our computer system sometimes it also effect the hard disk , and also sometimes it stole the data from our your system and send to others. A computer virus is a piece of software which attaches itself to another program causing inadmissible effect on the program. Based on the supplied survey the result indicated that viruses can infect computer system through a number of ways such as exchange of flash drive, hard disk and network medium. This paper contains an overview of the computer virus that can help the reader to evaluate the threat that computer viruses pose. The extent of this threat can only be determined by analyzing many different factors. Based upon the research, the development of a computer virus seems to require more persistence than professional experience. Recommendations are made to assist computer users in preventing bug by computer viruses. These recommendations support general computer security practices as a means of warring to computer viruses.**

***Index Terms*—Computer, Virus, flash drive, hard disk and network medium, computer security**

I. INTRODUCTION

The first computer virus, called "Creeper system", was an beginning of self-replicating virus released in 1971. It's working was like it take up the hard drive until a computer could not operate any further. The first computer virus for MS-DOS was "Brain" and was liberated in 1986. It would duplicate the boot sector on the floppy disk and prevent the computer from booting. It was written by two brothers from Pakistan and was initial designed as a copy protection. [1]

"The Morris" was the first Computer virus which spread broadly in 1988. It was written by Robert Morris, a graduate student from Cornell University who needed to determine the size of the internet. His approach used contract holes in send mail and other UNIX applications as well as weak passwords, but due to a programming mistake it spread too fast and started to interfere with the natural process of the computers. It contaminated around 15,000 computers in 15 hours, which back then was most of the internet.

The Internet worm of November 2, 1988, was one of the oldest computer worms distributed via the Internet, and the first to gain spotlight. It also resulted in the first breach conviction in the US under the 1986 Computer Fraud and Abuse Act. [3] . A computer virus is a type of malware that attaches to another program (like a document), which can recreate and spread after a person first runs it on their system. For instance, you could receive an email with a malicious attachment, open the file unknowledgeable, and then the computer virus runs on your computer. [5]Viruses are harmful and can destroy data, slow down system resources, and log keystrokes. The attention of virus free computer system cannot be over looked due to many factors surrounding and simplify system management such as cost of implementing a computer based information system, cost of association data, processing it and producing a meaningful information, risk of losing vital information and lots more. [7] Viruses therefore constitute a reasonable percentage of various threats that computer based information system faces. In fresh time, especially in the early part of 21st century, the word virus was strictly associated with the state of health of human beings i.e. the biological virus. Nowadays the word comes up both in biological and health sciences as well as computer sciences. However, it is well-known in the computer field as "computer virus". In the field of computer science, its effect cannot be disabled. [9]

Priya Bhargava, B.Tech Scholar, Dept. of CSE, Vivekananda Institute of Technology, Jaipur, Rajasthan
Rahul Choudhary, B.Tech Scholar , Dept. of CSE, Vivekananda Institute of Technology, Jaipur, Rajasthan
Ankesh Gupta, Assistant Professor, Department of CSE, Vivekananda Institute of Technology, Jaipur, Rajasthan

II. HISTORY OF VIRUS

1949, John von Neumann and "self-replicating machines" It was in those silver age of computing that mathematician, engineer, and polymath John von Neumann delivered a lecture on the Theory and Organization of Complicated Automata in which he first argued that computer programs could "self-reproduce. [16].

1982, the protocomputer-virus. In 1982 a fifteen-year-old boy was playing with his friends proved Neumann's theory a reality. Rich Skrenta's Elk Cloner is broadly regarded as the first proto-computer virus. Elk Cloner targeted Apple II computers, causing doctored machines to display a poem from Skrenta: Elk Cloner: It will get on all your disks. It will infiltrate your chips Yes, it's Cloner! It will stick to you like glue. It will convert RAM too Send in the Cloner!

Other notable firsts—Elk Cloner was the first virus to spread via severable storage media (it wrote itself to any floppy disk inserted into the computer). For many years to come, that's how viruses travelled across systems—via contaminated floppy disk passed from user to user[12].

1984, Computer virus, defined: In 1984 computer scientist Fred Cohen handed in his graduate paper defined computer virus , Computer Viruses – Theory and Experiments in which he coined the term "computer virus," which is great because "complicated self-reproducing robot" and it shocking for them . In the same paper, Cohen also gave us our leading definition of "computer virus" as "a program that can 'infect' other programs by modifying them to include a possibly evolved copy of itself."[10]

1986, the first PC virus: The Brain virus was the first to purpose Microsoft's text-based Windows precursor, MS-DOS. The plan of Pakistani brothers and software engineers, Basit and Amjad Farooq, was to make Brain acted like an early form of copyright protection, stopping people from pirating their heart monitoring software. If the target system composed of a pirated version of the brother's software, the "victim" would receive the message, "WELCOME TO THE DUNGEON . . . CONTACT US FOR VACCINATION" along with the brothers' names, phone number, and twin address in Pakistan. Other than guilt tripping victims in to paying for their pirated software, Brain had no harmful effects. [7]

1988, Computer virus of the year: 1988, one could dispute, was the year computer viruses went mainstream. In September of that year, a story on computer viruses arose on the cover of TIME magazine. The cover image delineated viruses as cute, googly eyed cartoon insects crawling all over a desktop computer. "Viruses were all about peace and love—until they started unmitigated people's computers."[2]

1988, front page of The New York Times
A little closed a month after the TIME magazine piece, a story about the "most funny computer 'virus' attack" in US ancient times appeared on the front page of The New York Times. It was Robert Tappan Morris' Internet worm, mistakenly referred to as a "virus." In all honor, no one knew what a worm was. Morris's creation was the archetype. The Morris worm thrown out more than 6,000 computers as it spread across the ARPANET, a government executed early version of the Internet restricted to schools and military installations. The Morris worm was the first well-known use of a dictionary attack. As the name propose, a dictionary attack involves taking a list of words and using it to try and guess the username and password aggregate of a target system [4].
Robert Morris was the first person charged under the newly authorized Computer Fraud and Abuse Act, which made it illegal to mess with government and financial systems, and any computer that contributes to US commerce and communications. In his shelter, Morris never advised his namesake worm to cause so much damage. According to Morris, the worm was designed to test security flaws and conclusion the size of the early Internet. A bug caused the worm to infect targeted systems over and over again, with each subsequent infection consuming processing power until the system crashed [6].

1989, Computer viruses go viral: In 1989 the AIDS Trojan was the first sample of what would later come to be known as ransomware. Victims received a 5.25-inch floppy disk in the mail labeled "AIDS Information" containing a simple questionnaire designed to help recipients figure out if they were at risk for the AIDS virus (the biological one).While an apt (albeit insensitive) metaphor, there's no indication the virus' creator, Dr. Joseph L. Popp, advised to draw parallels between his digital creation and the deadly AIDS virus. Many of the 20,000 disk recipients, Medium reported, were association for the World Health Organization (WHO). The WHO previously refused Popp for an AIDS research position. Unlike the Brain virus, however, the AIDS Trojan encodes the victims' files. [8]

1990s, Rise of the Internet: By 1990 ARPANET was decommissioned in favor of its public, commercially accessible cousin the Internet. And gratitude to Tim Berners-Lee's pioneering work on web browsers and web pages; the Internet was now a user-friendly place anyone could explore without special technical knowledge. There were 2.6 tons users on the Internet in 1990, according to Our World in Data. By the end of the decagon, that number would surpass 400 million.
With the rise of the Internet came new ways for viruses to spread. [10]

1999, "You've got mail (and also a virus)"
Think back to 1999. If someone you have sent you an email that read "Here is the document you demanded ... don't show anyone else," you opened the attachment. This was how the Melissa virus spread and it played on the public's openness about how viruses worked up to that point. Melissa was a macro virus. Viruses of this type cache within the huge language commonly used in Microsoft Office files. Opening up an energetic Word doc, Excel spreadsheet, etc. triggers the virus. Melissa was the fastest spreading virus up to that point, infecting approximately 50,000computers, Medium reported. [12]

2012, A full Shamoon over Saudi Arabia
By the turn of the 21st century, the map for future malware threats had been set. Viruses brick the way for a whole new generation of toxic malware. Cryptojackers covertlyused our computers to mine cryptocurrencies like Bitcoin. Ransomware held our computers hostage. Banking Trojans, like Emotet, stole our financial information. Spyware and keyloggers shoulder surfed us from across the web, stealing our usernames and passwords. [14]
Regular viruses were, for the most part, a thing of the past. In 2012, however, viruses made one last capture at the world's attention with the Shamoon virus.

Shamoon address computers and network systems belonging to Aramco, the state-owned Saudi Arabian oil company, in return to Saudi government policy arrangement in the Middle East. The attack stands as one of the most destructive malware attacks on a single organization in history, completely wiping out three-quarters of Aramco's systems. [16]

We have heard many terms such as virus, malware, Trojan, worm, ransomware, rootkit, software bug and now let's see what are these and how they are different from computer virus
Malware and Virus are mostly considered to be the same thing and people generally tend to interchange their meaning. Thus, it is important for one to know the discrepancy between malware and virus as these two terms are technically different from each other. Malware could be a form of malicious software which intends to infect the host computer. Whereas, Virus could be a sort of malware itself. It infects files so spreads through a tool whenever the file or program is run.

Malware and virus aren't the identical things. It's designed to induce unauthorized access to a system, generally for a 3rd party benefit. On the opposite hand, a virulent disease may be a code which attaches itself to numerous files and programs which get infected in a very manner that they will disrupt and

corrupt a tool [4]. The complete variety of Malware is Malicious Software, while that for Virus is important Information Resource under Seize Antivirus is accustomed remove an endemic from a computer device. An antivirus is intended to get rid of an infection from any device. It's not necessary for removing the virus only, but can also remove malware from a tool [15].

III. LITERATURE REVIEW

Some of the famous viruses of the digital age
In 1991, the "Michelangelo" virus was first discovered in Australia. It'd lay dormant until 6th March once a year so overwrite the first 100 sectors on the storage devices with zeros, preventing the pc from booting. Only 20,000 computers were reported infected. [11]

In 1998, "CIH" was released. It infected around 60 million computers and caused significant damages by overwriting important system files. It had been written by a Taiwanese student [13].
In 1999, "Melissa" was released. This one, was the first wide spread Word Macro Virus. It absolutely was distributed via email and would automatically send itself to the first 50 people within the Outlook address book. It didn't harm the pc because it absolutely was sending out passwords for some erotic websites which required membership. It caused such plenty email traffic resulting in email servers to crash [15].

In 2000, was the year of "iloveyou". Again, it came via email however it sent itself to any or all contacts. It also overwrote office, image, and audio files. The virus came from the Philippines and infected over 50 million computers in but 10 days. Most companies within the past decided to point out their email servers to forestall spreading the virus [5].

Since 2000, such plenty of latest viruses are unleashed to wreak havoc on the world at large that it's difficult to list the foremost. "Anna Kournikova", Code Red, Nimba, Beast, SQL Slammer, Blaster, Sobig, Sober, MyDoom, Netsky, Zeus, Conficker, Stuxnet, CryptoLocker, Locky, Mirai and WannaCry, are some examples that come to mind.

In 2013 the new kind of ransomware started with the CryptoLocker virus. There are many new versions of this virus including Locky and WannaCry, furthermore as Petya . The primary CryptoLocker virus infected about 1,000,000 computers in its original version. Variety of these clones, likeTorrent Locker or CryptoWall, were specifically designed to specialize in computers in Australia.

NotPetya exploited the identical security hole. It had been not delivered through email however, and then only had a limited reach. Initially it had been assumed that this virus may be an upgraded version of Petya, a CryptoLocker type ransomware. In fact, NotPetya was distributed as an updated version of a Ukrainian tax accounting package called MeDoc, and from there, it started spreading through internal networks of multinational companies with offices in Ukraine. It'd encrypt all files on a computer further because the most file table of a tough drive, preventing the pc from booting.
Now we've seen the famous virus which we will see how it came into existence which implies us look into the history of the computer viruses.

IV. VIRUS VS. MALWARE

The terms "virus" and "malware" are often used interchangeably, but they're not the identical thing. While a computer virus could also be a sort of malware, not all malware are computer viruses.
The easiest thanks to differentiate computer viruses from other styles of malware is to give some thought to viruses in biological terms. Take the flu virus, as an example. The flu requires some reasonably interaction between two people—like a hand shake, a kiss, or touching something an infected person touched. Once the flu virus gets inside a person's system it attaches to healthy human cells, using those cells to form more viral cells.

A malicious program works in much the identical way:

A bug requires a number program.

A computer program requires user action to transmit from one system to a different.

A bug attaches bits of its own malicious code to other files or replaces files outright with copies of itself.
It's that second virus trait that tends to confuse people. Viruses can't spread without some style of action from a user, like opening up an infected Word document. Worms, on the opposite hand, are ready to spread across systems and networks on their own, making them far more prevalent and dangerous.
Famously, the 2017 WannaCry ransomware worm spread round the world, took down thousands of Windows systems, and raked in an appreciable amount of untraceable Bitcoin ransom payments for the alleged North Korean attackers.

Is a Trojan a virus?

Trojans are often viruses. A Trojan could be a worm pretending to be something it's not for the needs of sneaking onto your computer and delivering some type of malware. To place it differently, if a scourge disguises itself then it's a Trojan. A Trojan may well be a seemingly benign file downloaded off the net or a Word doc attached to an email. Think that movie you downloaded from your favorite P2P sharing site is safe? What this "important" tax document from your accountant? Consider, because they might contain a pandemic. [14]

Is a worm a virus?

Worms aren't viruses, though the terms are sometimes used interchangeably. Even worse, the terms are sometimes used together in a very strange and contradictory word salad; i.e. a "worm virus malware." It's either a worm or an outbreak, but it can't be both, because worms and viruses discuss with two similar but different threats. A scourge needs a bunch system to copy and a few style of action from a user to spread from one system to the following . A worm, conversely, doesn't need a number system and is capable of spreading across a network and any systems connected to the network without user action. Once on a system, worms are known to drop malware or open a backdoor. [13]

Is ransomware a virus?

Ransomware is an outbreak. If so, then it's a ransomware virus. In fact, the very first ransomware was a plague. Nowadays, most ransomware comes as results of computer

worm, capable of spreading from one system to the following and across networks without user action.

Is a rootkit a virus?

Rootkits aren't viruses. A rootkit may be a software package designed to present attackers "root" access or admin access to a given system. Crucially, rootkits cannot self-replicate and don't spread across systems [9].

Is a software bug a virus?

Software bugs don't seem to be viruses. While we sometimes see a biological virus as a "bug" (e.g. "I caught a stomach bug"), software bugs and viruses aren't the identical thing. A software bug refers to a flaw or mistake within the coding system that a given software program is created from. Software bugs can cause programs to behave in ways the software manufacturer never intended. The Y2K bug famously caused programs to display the incorrect date, because the programs could only manage dates through the year 1999. After 1999 the year rolled over just like the odometer on an old car to 1900. While the Y2K bug was relatively harmless, some software bugs can pose a heavy threat to consumers. [8]

General Behavior of Computer Viruses

Computer viruses behave substantially like their biological counterparts. The American Heritage Dictionary of a people Language defines an outbreak as: Any of varied submicroscopic pathogens consisting essentially of a core of one super molecule surrounded by a protein coat, having the power to duplicate only inside a living cell. Any specific pathogen. Something that toxins one's soul or mind. The important a part of this definition is that a scourge is capable of replicating itself. Also note that replication is feasible only within the presence of a "living" host, which differentiates a scourge from a worm. Both of these points carry over well to computer viruses. They are lf-replicating and want a bunch system to survive.

V. Phases of Virus Infection Computer

Viruses generally labor less than four unique phases during the course of their existence in an exceedingly automatic data processing system. [7]
These phases are as follows:

1. Dormancy phase
2. Propagation phase
3. Triggering phase
4. Damaging phase

During the dormancy phase, the user is also lulled into believing that the software containing the virus is safe. The OS of the pc is infected, but no additional damage is inflicted during this phase, and therefore code doesn't propagate itself to other software. The Macintosh SCORES virus lies dormant for two calendar days before getting to the following phase. [11]

The propagation phase is that only phase necessary for a program to be labeled a pandemic. During this phase, the virus attempts to connect itself to other applications or data files within the system. The most purpose is to possess the attached viral code executed before to the execution of the infected software. Once the code is attached to other software, it should be spread to other machines via the transfer of floppy disks or across a network. [15]

The triggering phase determines when verity purpose of the virus is revealed to the user. Like logic bombs, the triggering mechanism is restricted only by the imagination of the software author. Common mechanisms are supported the date and time, the quantity of times the virus has replicated itself, or the amount of executions since infection. Finally, the virus performs its intruded purpose [8].

Among other damaging features, when triggered, this virus will delete any applications that are executed. However, the aim isn't always so obvious. Once again, the damage is - limited only by the imagination. By changing bits of knowledge in sensitive areas of memory, the system is created to exhibit erratic behavior. By changing bits within a spreadsheet file, the spreadsheet may now not be used or could contain erroneous information [16].

Anatomy of a Typical Virus

As stated previously, a program must be ready to propagate itself to be considered a deadly disease. This really the sole requirement to propagate, the virus must attach itself in a way to the operating environment of the pc. Once attached, the virus is then liberal to infect other applications. These applications may then be carried on floppy disks to other computers, or the application is also run on other machines across a neighborhood area network (Figure 1). Either way, the applications then can infect other operating systems, and also the cycle continues. There, must be this two-way infection process: system -> application and system <- application. [5]

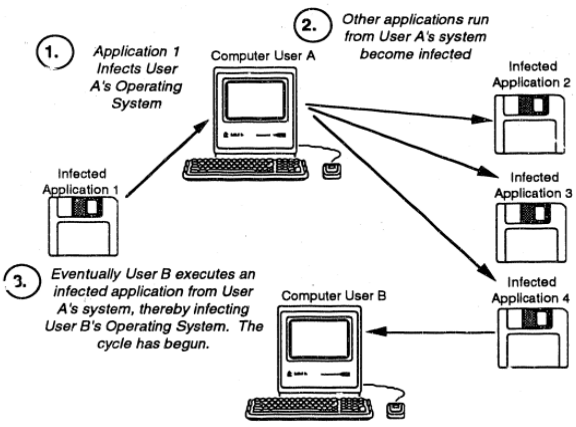

Fig.1: Example of Virus Propagation

System -> Application Infection

Because the act of virus propagation is circular in nature, any discussion of the method must begin by assuming that either the system or the appliance is already infected. For this discussion, it's first assumed that the OS is already infected by a virulent disease. [2] The first, purpose when infecting an application is to urge viral code executed a while during the execution of the application. The viral code is often destructive or nondestructive, and it should incorporate a dormancy phase but at some point it'll always try and propagate the virus. Assume that the OS of a computer has

become infected by a malicious program. The primary step in propagating the virus is to choose when to focus on and infect applications. Some viruses attack as soon as a diskette is inserted into the disk drive; some attack while an uninfected application is executing; others may simply attack willy-nilly. The following discussion shows how a "typical" computer program can propagate through an automatic data processing system. Of course, this can be not the sole way that an epidemic can propagate, but it does function a decent example. Figure 2 illustrates how a traditional software system call may be implemented. [9] The particular operational details of this call are omitted from this paper. [16]

Figure 3 shows how a virulent disease can be able to infiltrate a software package. Notice that viral code is now being executed within the execution cycle of the program.

Application -> System Infection

The idea made above was that a software system had somehow been remapped to point to viral code. This section will describe how that would be accomplished. [11]

When an infected application is executed, the viral code gains control. This code then attempts to infect the package of the pc on which it's executing. If it's determined that the software is already infected, no action is taken. If the system isn't already infected, it are often infected by inserting code into the software system specified this code are executed at startup or another predetermined time [6].

The purpose of this inserted viral code is to remap one or more of the software calls (as seen in Figure 3). This completes the virus cycle of infection. The software system infects applications, and applications in turn infect operating systems.

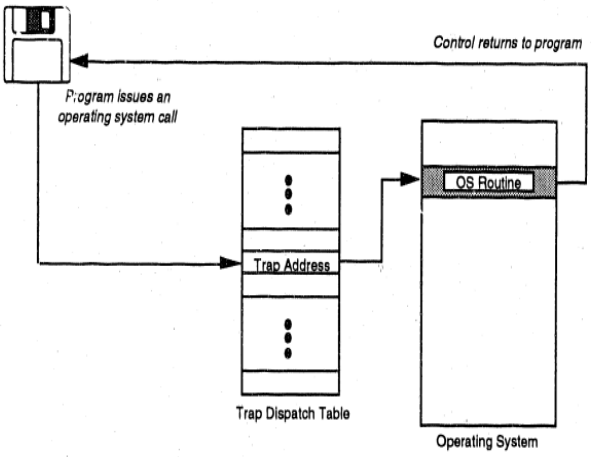

Figure 2. Normal Operating System Call.

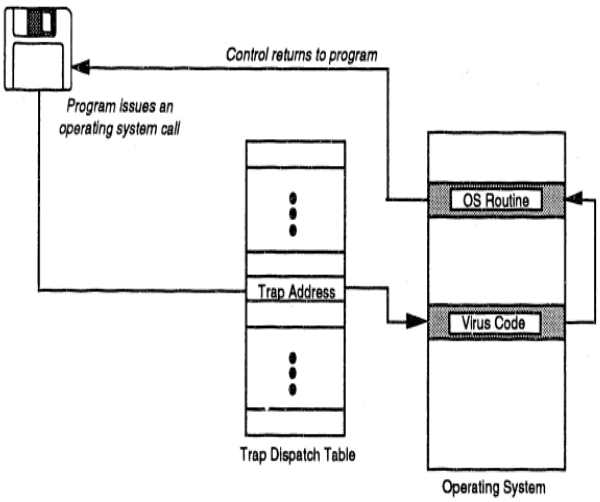

Figure 3. Redirected Operating System Call.

VI. Conclusion

Through this paper we able to know what's the computer virus. How it came into existence and the way by year and year it become difficult for us handle it and also how it add the system and also we are able distinguish between the virus, malware , Trojan , system bugs and other things . There's certainty that the long run will witness the event of more sophisticated codes for viruses. These viruses are also difficult to detect and if detected, could prove stubborn to erase or remove from the computer system. This may now not be seen as malicious act but as significant impact on the long run of computing, knowing well that viruses are legitimate software. It becomes an intellectual challenge to become an outbreak and antivirus developer. This might in a way or the opposite limit the expansion of knowledge technology thanks to fear of loss of capital to the users. Many folks may opt to give-up the fate they'd on system. So as to assist people stand the test of your time, the researcher has considered this research study as how of exposing viruses and its characteristics to the broader world. Implementing the advice obtained during this study will go protected thanks to prepare both the pc experts and users for the long run war against viruses, which can defile even the employment of weapons like as antivirus. Implementing antivirus software might be expensive considering compatibility of some antivirus to the prevailing hardware and software, but the advantages outweigh its cost. Information as an excellent tool for management decision must be secured. The subsequent are recommendations: mortal is inspired to report every virus attack they encounter to computer specialists so on make materials available for upgrading the present antivirus and writing new ones; it absolutely was carefully observed within the course of this research work, that when users delete a plague from a component, they have an inclination to forget that the virus may need infected one or two other components apart from the one seen, thus giving room for the virus to pick up which (to the user) is caused by inefficiency of the antivirus, but on no account. The user only must ensure that each drives and diskettes are properly scanned at any suspicion.

REFERENCES

[1] Collins, H. 1990. The Computer Virus Protection Handbook. Arnold Ltd London.

[2] Solomon, A. and Dmitry, O. 1994. Dr. Solomon's Virus Encyclopedia. 3rd Edition. S & S International. Berkhamsted, London.

[3] Gram, J. 1998. Windows Internet Server 4 (second edition) University of North Carolina.

[4] Jan, A. 1993. Computer Virus and Antivirus Warfare (2nd Revised). Hemstend Ellis Horwood.

[5] Kaushik, S. Pang Diwan 1990. Information Technology (tenth edition) University of Essex. Associates, 4423

[6] Shoch J. & Hupp J. The 'worm' programs? early experience with a distributed computation. Communications of ACM, Volume 25, pp. 172-180, March 1982.

[7] Brien, J. A. O. 1996. Management Information System (third edition) University press New York.

[8] John, D. Macfee 1987. Computer Industry Association Microsoft (second Edition) academic press New York.

[9] Aryen, G. 1999. Quick Start Instruction for McAfee Associates Programs. McAfee.

[10] Snorre, F., Sylvia M., Kenneth, W., and Carl, B. 2003. The Norman Book on Viruses. Helsinki Inc. Switzerland.

[11] Solomon and Gyaznor 1984. Research manual (third edition) University press New York.

[12] Cheeney Street, Santa Clara, USA.

[13] French, C. S 1996. Data Processing and Information Technology (tenth Edition) University of Oxford press Oxford.

[14] S.U. Jen 2002. Fundamentals of Research Methodology. 1st Edition. Paraclete Publish

[15] Fred Cohen in 1983.

[16] American Heritage Dictionary of the English Language, Copyright 1985, Houghton Mifflin Company, Boston, Massachusetts, p. 1351.