A Study on Hazards of Computer Viruses

Jaishma Kumari B[1], Sathwik U Shetty[2], Pushvin Gowda[3], Nisha Tellis[4]

Assistant Professor, Department of Information Science and Engineering[1]

Students, Department of Information Science and Engineering[2,3,4]

Alva's Institute of Engineering and Technology, Mijar, Mangalore, Karnataka

Abstract: *Computer use is becoming part of our lives every other day however there have been considerable threats of computer viruses in the recent past. Viruses have had adverse effects on data and programs ranging from formatting hard disks, damaging information infrastructure, suddenly restarting machines, deleting or modifying data and in some cases mild effects such as slowing down machines or producing irritating sounds. Viruses have been a major cause for worry especially with the advances in data processing, storage and movement of information technologically. Many computer users and organizations especially the computer intensive organizations have had to invest heavily in dealing with viruses particularly those organizations running the windows platform. These computer viruses have been defined by their characteristics of entry and multiplication without the user's notice as well as diverting the normal functioning of the computer. This paper seeks to define a virus and explain its related terms such as malicious software, worms, and Trojan horses. It explains vulnerabilities of operating systems in relation to viruses, it makes an observation on strengths of Linux versus Windows, outline the present state of affairs, apart from using anti-virus software, there are other procedures which can help protect against viruses which are also mentioned, the future of computer viruses and the conclusion that the Internet is serving its purpose of interconnecting computer and hence promoting distribution of viruses then makes some recommendations on viruses.*

Keyword: Computer Virus, Malware, Operating Systems.

I. Introduction

A day as information security researchers reveal new threats and security vulnerabilities in the technologies Computer viruses are software programs that are designed and developed to interfere with normal computer operations and spread from one computer to another without the operator's knowledge. Computer viruses fall in the family of malicious programs which are otherwise called malware. Malware also includes rootkits, spyware, worms, Trojan horses and fraudulent adware. According to O'Donnell (2012), a rootkit is a silent type of malicious software designed to hide the survival of some processes from the standard methods of detection and enables illegal access to a computer. According to Wienbar (2005), Spyware is a type of malware that gathers information about users in a computer exclusive of their awareness. The existence of spyware is concealed from the user and can be difficult to notice. Oldfield (2005) defines a worm as a malicious program that exploits security vulnerabilities to extend to new computers through network and a Trojan horse as a program that shows undisruptive characteristics but conceals its malicious capability. Viruses exploit some system vulnerabilities whether in operating systems or some application software to get illegal rights of entry, harm other programs, and do damage to user operations or user data. Viruses in the early years did spread slowly this was because they were mostly on floppies, but the evolution of computer networks and the internet has made spread easier and more rapid. The paradox is the more connected a country or an organization is, the more vulnerable it is to viruses.

Cyber security is the biggest concern in today's world. This threat is increasing each that are widely used, which puts the security at a higher risk [1]. The number of network attacksis at its highest level in last few years, the biggest threat to any computer system is computer virus which proves itself to be the most devastating and the most commonly found

DOI: 10.48175/IJARSCT-2107

technique to compromise systems. Moreover, investigating a various security features [2-4] could be an interesting path to explore in the future to protect Big Data [5]. This research paper will address these threats and we will try to find out its operations and types of attacker who can use these tools to compromise the security system.

Finally, we will discuss the tips and techniques that can prevent us from being infected by these malicious and sophisticated computer viruses. Computer viruses are basically a computer code which is capable of copying itself to other files and performs the required tasks mentioned in it codes. Virus is the most commonly used terminology in discussions due to its nature. The most appropriate term we can use is self-replicating programs because in the beginning the intensions were to create an artificial intelligent program nonetheless later it was changed for different purposes. There are number of viruses which have their own purpose and propagation techniques [1]. The basic routines that are normally used in computer viruses, are as follows. Functional diagram of a computer virus, which has search, copy and anti-detection routines to avoid any detection from anti-virus software representing the number of updates that Avast anti-virus software provides to its users which is increasing every month. databases getting new and more data about computer viruses every month which should be shared with every user to prevent them from any newer thearts.

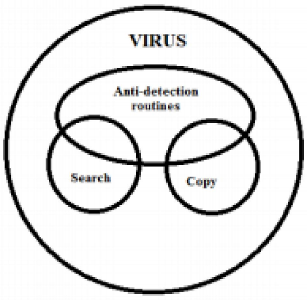

Figure 1. Functional diagram of a computer virus, which has search, copy and anti-detection routines to avoid any detection from anti-virus software

II. Information about Virus

A computer virus is self replicating program containing code that explicitly copies itself and that can infects other program by modifying then or their environment .Harmful program code refers to any part of programme code which adds any sort of functionality against the specification. A virus is a program which is able to replicate with little or no user intervention, and the replicated program(s) are able to replicate further. Malicious software or malware for short, are "programs intentionally designed to perform some unauthorized - often harmful or undesirable act." Malware is a generic term and is used to describe many types of malicious software, such as viruses and worms. A typical structure of a computer virus contains three subroutines. The first subroutine, infect-executable, is responsible for finding available executable files and infecting them by copying its code into them. The subroutine do-damage, also known as the payload of the virus, is the code responsible for delivering the malicious part of the virus. The last subroutine, trigger-pulled checks if the desired conditions are met in order to deliver its payload.

The structure of Computer Virus can be divided into four phases;

A. Mark cans prevent re-infection attempts.
B. Infection Mechanism causes spread to other files.
C. Trigger is conditions for delivering payload.
D. Payload is the possible damage to infected computers.

III. History Of Computer Virus

There are thousand and thousand of different viruses these days which improve every day. However, there is much software released every day to detect and avoid these viruses. Although the wild spread of new and strong viruses, it

DOI: 10.48175/IJARSCT-2107

still infects and spread only with user's permission. There are endless arguments about the "first" virus. There were a number of malware attacks in the 1970s and some count these among the virus attacks. The description of the malware, however, would indicate these were worms and not viruses by general definition. Just to be complete, however, the questionable entries from the 1970s are included here with that Computer Knowledge considers virus history to start in 1981. And in year 1995 to 2000 the total number of computer virus are created. And in 2001 to 2010 them are increases up to 1221 number of newly create computer virus. The new computer virus are created from year 2005 to year 2010 are shown in table 1. The table shows that for every month computer virus are created.

IV. Working of Computer Virus

Computer viruses have a life cycle that starts when they're created and ends when they're completely eradicated. The following diagram [Diagram 1: Life Cycle] points are .

- **Stage I - Creation**– The Computer viruses are created by misguided individuals who wish to cause widespread, random damage to computers.
- **Stage II -Replication -**Computer Viruses replicate by nature means it copies itself from one PC to anther PC.
- **Stage III -Activation -**Viruses that have damage routines will activate when certain conditions are met. Viruses without damage routines don't activate, instead causing damage by stealing storage space.
- **Stage IV -Discovery -**This phase doesn't always come after activation, but it usually does. Discovery normally takes place at least a year before the virus might have become a threat to the computing community. Stages V -Assimilation - At this point, antivirusdevelopers modify their software so that it can detect the new virus. This can take anywhere from one day 13
- **Stage VI -Eradication -** If enough users install up-to-date virus protection software, any virus can be wiped out. So far no viruses have disappeared completely, but some have long ceased to be a major threat. The same or different developer develops a different strain of a new virus and process begins afresh.

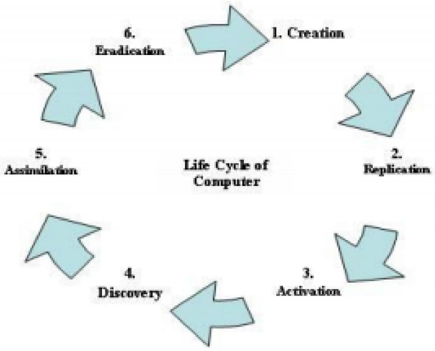

Diagram 1: Life Cycle Of Computer Virus

4.1 General Symptoms of Viruses

The following are some symptoms of virus infections in your computer system:

- Some system files may be missing or you receive error messages on missing files.
- The computer functions as anticipated but at other times, it stops responding.
- The operating systems may not start although you may not have done any installations or modified any programs.
- The computer takes longer than expected to run an application.
- Computer programs may stop acting in response frequently.
- Computer hard disk partitions disappear.
- The computer may also crash.

- The computer may come to a halt when you try to use Microsoft Office objects.
- Whenever you cannot start or run the Windows Task Manager.
- When antivirus software detects the presence of a computer virus.
- Disk drives and disks may be inaccessible to users.
- There is a twofold extension on documents you lately opened such as .doc.exe.
- An antivirus program is disabled for no reason.

Additionally, the antivirus program cannot be restarted.

4.2 Current Trends of Viruses

There is a new spot of anxiety in viruses which was first identified in 2007 of cross-platform malware. This has been greatly inspired by the attractiveness of cross-platform computer applications. This was brought to the forefront of malware awareness by the circulation of an OpenOffice.org virus named bad bunny. Smith S (2007) of Symantec comments on this cross platform viruses that scripting platforms, extensibility, plug-ins, ActiveX can be used. There is a trend in Linux to malware that deceives the user to install a malicious software. This is often referred to as social engineering for example in 2009 a malicious screensaver called the waterfall was exposed which included a script to run some attack to deny users some services. In future viruses may not be limited to computers since there is spread use of microchips to support human health and biometric features, there may be newer versions of viruses which will affect these chips as argued by Warwick (2004). It is also expected that viruses will be able to spread far and wide especially when powerful processors find their way into household electronic appliances such as Televisions and microwaves. Malicious code or viruses can be used in future as a cyber weapon to penetrate a country's dangerous information infrastructure or for intelligence reason to spoil the infrastructure. The results may be:

- Destroying critical control systems such as those used in airports. Damaging the national telecommunication systems infrastructure.
- Demolish financial information systems used in banking. Shutting down the control systems used in electrical distribution.

V. Common Types of Computer Viruses

1. **Resident Virus:** Resident viruses set up shop in your RAM and meddle with your system operations. They're so sneaky that they can even attach themselves to your anti-virus software files.
2. **Multipartite Virus:** This virus infects the entire system. Multipartite viruses spread by performing unauthorized actions on your operating system, folders, and programs.
3. **Direct Action:** This virus targets a specific file type, most commonly executable files (.exe), by replicating and infecting files. Due to its targeted nature, this virus type is one of the easier ones to detect and remove.
4. **Browser Hijacker:** Easily detected, this virus type infects your browser and redirects you to malicious websites.
5. **Overwrite Virus:** Like the name implies, overwrite viruses overwrite file content to infect entire folders, files, and programs.
6. **Web Scripting Virus:** This sneaky virus disguises itself in the coding of links, ads, images, videos, and site code. It can infect systems when users download malicious files or visit malicious websites.
7. **File Infector:** By targeting executable files (.exe), file infector viruses slow down programs and damage system files when a user runs them
8. **Network Virus:** Network viruses travel through network connections and replicate themselves through shared resources.
9. **Boot Sector Virus:** One of the easier viruses to avoid, this virus hides out in a file on a USB drive or email attachment. When activated, it can infect the system's master boot record to damage the system.

5.1 Solutions

Apart from using anti-virus software, there are other procedures which can help protect against viruses some of which include:- Running scheduled, updated virus scan software on all computers within the organization at least once a week. Keeping software patches updated with some updates such as windows systems updates which can be downloaded from vendors' websites. Permit only approved software to run on your institution so that unaccepted programs are not run. This involves revoking installation privileges from users so that they may not install any programs. Practice minimum privileges to users such that they only have access to what they need to carry out their day to day businesses especially on servers. Occasionally run vulnerability scanners from both inside and outside your network to find computers with vulnerabilities so you will know which ones need patched. Antivirus corporations should create software that averts cyber threats and involve policies which are government-backed to curb criminals involved in cyber-crime of creating and distributing viruses to make money from selling antivirus programs. Users should be advised to make regular backups for all data and programs such that if the systems are infected, it is possible to restore any lost programs and data.

A computer virus is software intentionally written to copy itself without the computer owner's permission and then perform some other action on any system where it resides. Now a days, viruses are being written for almost every computing platform Anti-virus protection is, or should be, an integral part of any Information Systems operation, be it personal or professional. There are number of computer virus are created and these computer virus are affected in day today life. These viruses erase important data. before finding the solution against the computer virus people must know the basic thing of computer virus like which are the type of computer virus are created now a days, working of computer virus, problem occurs from computer virus.

REFERENCES

[1]. Q. Zhu, X. Yang and J. Ren, "Modeling and analysis of the spread of computer virus", Communications in Nonlinear Science and Numerical Simulation, 17(12), pp. 5117-5124,2012.

[2]. D. V. Pham, M. N. Halgamuge, A. Syed P. Mendis, Optimizing windows security features to block malware andhack tools on USB storage devices, Progress in electromagnetics research symposium, pp. 350-355, 2010.

[3]. P. Szor, "The art of computer virus research and defense" ,Pearson Education, 2005.

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

[5]. **5.**Dr. Klaus Brunnstein 1999, from Antivirus to Antimalware Software

[6]. and Beyond http://csrc.nist.gov/nissc/1999/proceeding/papers /p12.pdf

[7]. Paul Royal, Mitch Halpin, David Dagon, Robert Edmonds, and Wenke Lee. PolyUnpack: Automating the Hidden-Code Extraction of Unpack-Executing Malware. In The 22th Annual Computer Security Applications Conference (ACSAC 2006), Miami Beach, FL, December 2006.

[8]. Rainer Link, Prof. Hannelore Frank, August, 2003, Server-based Virus-protection On Unix/Linux

[9]. Paul Oldfield (2004), Viruses and spam what you need to know. Sophos Plc

[10]. Wienbar, Sharon (2005), The Spyware Inferno. America Online & The National Cyber Security Alliance.

[11]. Waqar Ahmad (2003) Computer Viruses as a Threat to Home Users International Journal of Electrical & Computer Sciences King Abdul Aziz University Jeddah. Saudi Arabia.

[12]. Panda Security (2012),Microsoft Security Intelligence Report, Consumer Reports. Published Available online on http://www.statisticbrain.com/computer-virus-statistics

DOI: 10.48175/IJARSCT-2107