IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114152

COMPUTER VIRUS AND SECURITY

Sharayu Salunke, Sheetal A. Wadhai

Department of Computer Engineering, Universal College of Engineering and Research, Pune

Abstract: Today's enterprise networks are distributed to different geographical locations and applications are more centrally located, information represents the most important asset. With the growing number of data communication services, channels and available software applications, data are processed in large quantities and in a more efficient manner. This technological enhancement offers new flexible opportunities also measure security threats poses in the networks. These threats can external or Internal, external threats divided as hacking, virus attack, Trojans, worms etc. There are thousands and thousands of different viruses these days which improve every day. Although the wild spread of new and strong viruses, it still infects and spread only with user's permission. This research paper highlights the phases of computer virus, computer virus, history of worst computer attack, type of computer virus with effect on computer & few examples of virus on their types, working of computer virus, and problem occur due to virus in computers.

Keywords: Computer virus, types of virus, infected, antiviruses, security, security threats, hacking.

1. INTRODUCTION:

Increase in population and digitalization have increased the interest in computer virus. A virus is a computer program created to infect other programs with copies of itself. It has the ability to clone itself, so that it can multiply, constantly seeking new host environments (McAfee et al, 1989). Since a virus' goal is to get executed by the computer, it must attach itself to a COM, EXE or SYS file. (Ludwig , 1996).Mathematical models have been important tools in analyzing the transmission of virus (Roshan and Smita, 2017). Network analysis is powerful because of its breadth. By abstracting away the details of a problem and mapping it onto a network, we can describe the important topological features with a clarity that would be impossible were all the details retained (Newman et al, 2011). The computer virus impacted financial loss. The most damaging virus/worm is 'MyDoom' which caused $38 billion in damages by slowing global Internet access by 10% in 2004, 'Sasser' which brought down Delta Airlines and crashed millions of PCs to cause more than $18 billion in damages in 2008, 'ILOVEYOU' which ended up shutting down the US government's email servers and causing $15 billion in damages in 2000 (WebFX, 2014). In modern life, human intervention plays a significant role in preventing the breakout of computer viruses (Yang et al, 2012). The rest of the paper is organized as follows. Malicious objects details in section II , analysis of malicious objects research work from different research journals in section III , discussed the computer virus problems in section IV , comparison of computer virus Vs biological virus in section V, computer virus control methods in section VI , analysis of SIS and SIR model in section VII , timeline of computer virus in section VIII and Finally, this paper is summarized by a conclusion.

2. What is computer virus?

A computer virus is a program which can harm our device and files and infect them for no further use. When a virus program is executed, it replicates itself by modifying other computer programs and instead enters its own coding. This code infects a file or program and if it spreads massively, it may ultimately result in crashing of the device.

Across the world, Computer viruses are a great issue of concern as they can cause billions of dollars' worth harm to the economy each year.

Since the computer virus only hits the programming of the device, it is not visible. But there are certain indications which can help you analyse that a device is virus-hit. Given below are such signs which may help you identify computer viruses:

The first thing which you might notice in case of virus attack is the speed with which your system shall process. And then gradually other changes can also be observed.

3. History of computer virus

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

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114152

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

4. Types of computer virus

There are number of harmful programme code are rapidly infect large numbers of computer systems And which created day by day. Therefore, these harmful programme code can be divided in to Boot Sector Virus, Trojan Horses, File Infecting Virus, Micro Virus, Malicious Toolkits Computer Worms, Spyware, Joke program and logic bombs, computer viruses, Droppers, Injector and Germs, Memory – resident virus, Program File Virus, Polymorphic virus, E-mail

4.1 Memory Resident Virus

lodges in main memory as part of a resident system program. From that point on, virus infects every program that executes.

4.2 Program file Virus

infects programs such as Exe, Com and Sys – files. The following Figures show details.

4.3 Polymorphic Virus

creates copies during replication that are functionally Equivalents but have distinctly different bit patterns

4.4 E-Mail Virus

More recent development in malicious software is the e-mail Virus. The first rapidly spreading e-mail viruses, such as Melissa, made use of a Microsoft word macro embedded in an attachment. If the recipient opens the e-mail attachment, the word macro is activated then.

4.5 Malicious Tools

Are malicious programs designed to automatically create viruses, worms, or Trojans, conduct DoS attacks on remote servers, hack other computers, etc.

4.6 Boot Sector Virus

Boot sector viruses infect the Master Boot Sector of hard drives or floppy drives and infect other machines only when the machine boots up from an infected floppy disk. Boot Sector viruses were the first successful viruses created and can infect a machine regardless of what Operating Systems runs on it.

4.7 File Infecting Virus

Program viruses infect executable programs, such as EXE or COM, by attaching themselves to them. The virus executes and infects other executables when its host file is executed. To infect an EXE file, a virus has to modify the EXE Header and the Relocation Pointer Table.

4.8 Micro Virus

These viruses are written in macro languages and infect files that make use of the particular language. A macro is a series of steps that could otherwise be typed, selected, or configured, but is stored in a single location so they can be automated. Some programs are nothing than hundreds of macros build around vendors' applications. Macro languages are used to allow more sophisticated macro development and environment control, like manipulating and creating files, changing menu settings, and much more. Macro languages are so easy to use that virus writers can learn to write their first virus in a couple of days.

4.9 Spyware

Spyware is the name given to the class of software that is surreptitiously installed on a computer, monitors user

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114152

activity, and reports back to a third party on that activity.

4.10 Logic Bombs

Logic Bombs are rarely stand-alone programs. Most often, they are a piece of code embedded in a larger program, it initiates on a specific action.

4.11 Trojan Horses

A Trojan horse is a program which performs something useful; while in the same time intentionally performs, unknowingly to the user, some kind of destructive function.

4.12 Droppers: A dropper is a special kind of Trojan horse, the payload of which is to install a virus on the system under attack. The installation is performed on one or several infect able objects on the targeted system. Injectors: An injector is a program very similar to a dropper, except that it installs a virus not on a program but in memory.

4.13 Germs

A germ is a program produced by assembling or compiling the original source code of a virus or of an infected program

4.14 Worms

Programs which are able to replicate themselves as stand-alone programs and which do not depend on the existence of a host program are called computer worms.

4.15 Directory Virus

A directory virus functions by infecting the directory of your computer. A directory is simply a larger file that contains information about other files and sub-directories within it. The general information consists of the file or directory name, the starting cluster, attributes, date and time and so forth. When a file is accessed, it scans the directory entry in search of the corresponding directory.

4.16 Hacker

Computer hacking refers to gaining unauthorized access to, and hence some measure of control over, a computer facility, and most countries now have specific legislation in place to deter those who might wish to practice this art and science. However, in practice, hackers generally have a particular target in mind, so their unauthorized access leads to further acts, which national law might also define as criminal activities. These can be summarized under the headings of unauthorized: Obtaining of confidential Information, Alteration or deletion of data and Code, Degradation or cessation of Services, Use of computer resources.

5 Antivirus

Organization need to provide security skeleton to prevent the data hidding due to malicious code. In order to provide the security the organizations go through the security audit and most of the organization chose the internet security software as well as design their personal firewall and antivirus. Antivirus solutions are now a common component of computer system. However, security issues pertaining to the anti-virus software itself have not captured enough attention of anti-virus vendors and computer users. "Antivirus" is protective software designed to defend your computer against malicious software. Malicious software or Malware includes: viruses, Trojans, keyloggers, hijackers, diallers, and other code that vandalizes or steals your computer contents. Anyone who does a lot of downloading, or accesses diskettes from the outside world on a regular basis should develop an antivirus strategy. Antivirus software is equipped with features that not only check your files in your system, but also check your in-coming and out-going e-mail attachments for viruses and other malicious programs. The most important weapon in your antivirus is a clean, write-protected bootable system diskette. Booting from a clean write-protected diskette is the only way to start up your system without any viruses in memory. An effective defense against viruses is a clean backup of your hard drive. Many antivirus packages will attempt to disinfect infected programs for you so that the virus is no longer in your system. Antivirus products are categorised into three parts such as Internet Security [IS], Total Security [TS], and Antivirus [AV]. Antivirus: products are the products which are primarily focused on detecting and remediating viruses and spyware. Internet Security product provides all the virus and spyware removal features of an AV, as well as additional functions to provide greater Internet

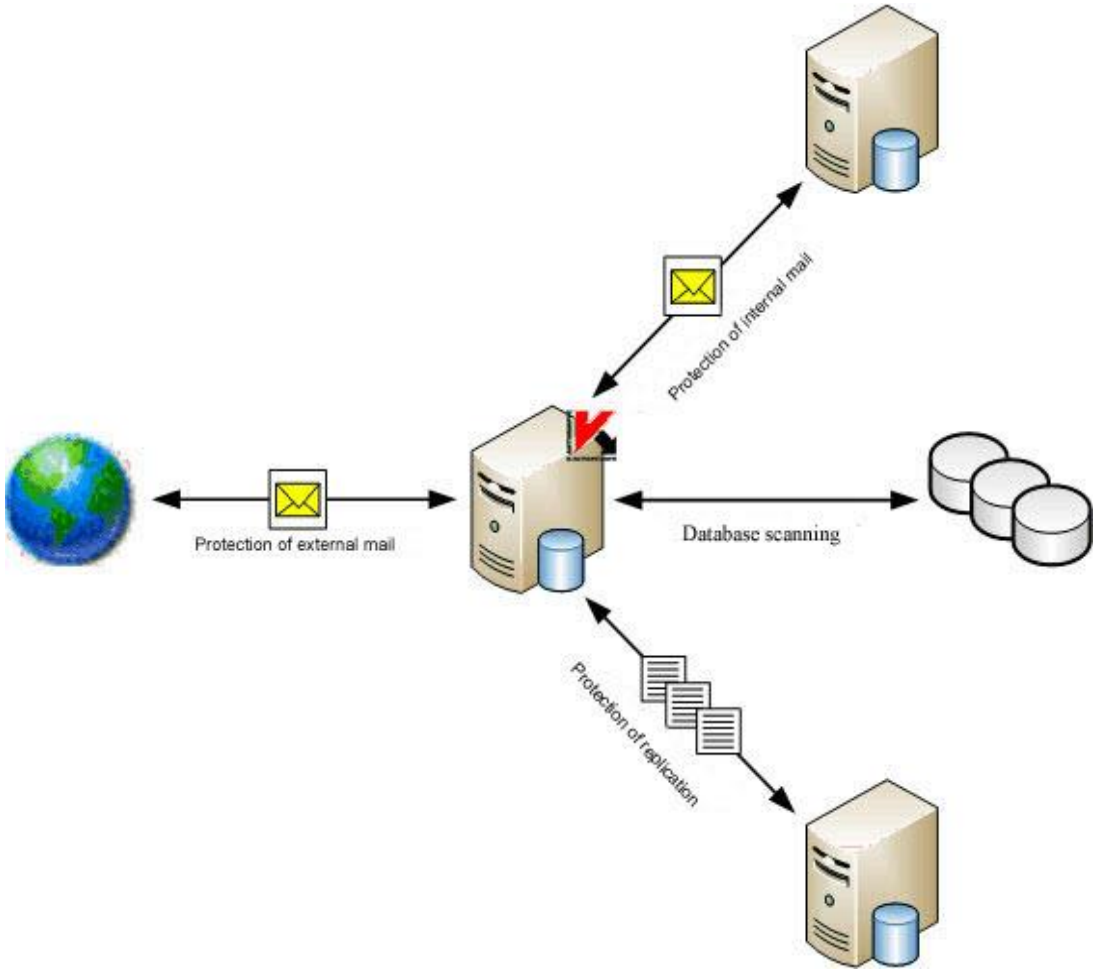
IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114152

protection. These features may include protection against phishing, root kit detection, firewalls and scanning of web pages and HTTP data. Total Security: products provide data migration and backup features on top of all security features common to IS products. Antivirus software is class of program that reaches a hard drives and floppy disk, pen drives for any known or potential viruses. It runs random access of memory of a computer. Anti-virus software typically uses two different techniques to accomplish this



6 Security threats

The terms threat, vulnerability and weakness are often used in cybersecurity. Understanding the difference between these terms is important. It allows organizations to correctly implement, document and assess their cybersecurity activities and controls. Here, we take a closer look at security threats**.** Cyber threats are sometimes incorrectly confused with vulnerabilities. Looking at the definitions, the keyword is "potential". The threat is not a security problem that exists in an implementation or organization. Instead it is something that *can* violate the security. This can be compared to a vulnerability which is an actual weakness that can be exploited. The threat always exist, regardless of any countermeasures. However, countermeasures can be used to minimize the probability of it being realized.

Types of security threats

The NIST definition above states that a threat can be an event or a condition. An event, in this case, also includes natural disasters, fire, and power outage. It is a very general concept. In cybersecurity, it is more common to talk about threats such as viruses, trojan horses, denial of service attacks.

Phishing emails is a social engineering threat that can cause, e.g., loss of passwords, credit card numbers and other sensitive data. Threats to information assets can cause loss of confidentiality, integrity or availability of data. This is also known as the CIA triad.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114152

The CIA triad, together with three other well known security concepts, is the basis for the STRIDE threat model. When listing possible threats, it is convenient to use an existing classification as a starting point. STRIDE is the most well-known classification, proposed by Microsoft in 1999. The name comes from the initial letters of the different categories, which also makes it easier to remember them.

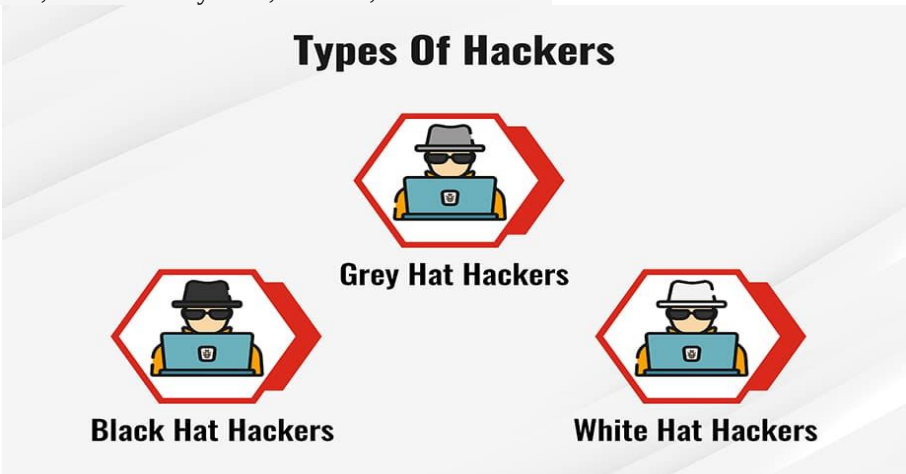
Threat	**Meaning/Example**	**Related Security Property**
Spoofing identity	An example is to use someone else's password and authenticate as that person.	Authentication
Tampering with data	This includes e.g., modification of data. Either data at rest or data sent over a network.	Integrity
Repudiation	This means that users can deny having performed an action, e.g., sending or receiving data.	Non-repudiation
Information disclosure	This includes a user reading data without granted access, or eavesdropping a communication channel.	Confidentiality
Denial of service	This relates to the availability of a system	Availability
Elevation of privilege	In these types of threats, a less privileged user gets higher privileges. Normal users obtaining root privileges is the most typical and severe form of this	Authorization

7 Hackings

A commonly used hacking definition is the act of compromising digital devices and networks through unauthorized access to an account or computer system. Hacking is not always a malicious act, but it is most commonly associated with illegal activity and data theft by cyber criminalsHacking refers to the misuse of devices like computers, smartphones, tablets, and networks to cause damage to or corrupt systems, gather information on users, steal data and documents, or disrupt data-related activityA traditional view of hackers is a lone rogue programmer who is highly skilled in coding and modifying computer software and hardware systems. But this narrow view does not cover the true technical nature of hacking. Hackers are increasingly growing in sophistication, using stealthy attack methods designed to go completely unnoticed by cybersecurity software and IT teams. They are also highly skilled in creating attack vectors that trick users into opening malicious attachments or links and freely giving up their sensitive personal data.As a result, modern-day hacking involves far more than just an angry kid in their bedroom. It is a multibillion-dollar industry with extremely sophisticated and successful techniques.

8 Types of Hacking/Hackers

There are typically four key drivers that lead to bad actors hacking websites or systems: (1) financial gain through the theft of credit card details or by defrauding financial services, (2) corporate espionage, (3) to gain notoriety or respect for their hacking talents, and (4) state-sponsored hacking that aims to steal business information and national intelligence. On top of that, there are politically motivated hackers—or hacktivists—who aim to raise public attention by leaking sensitive information, such as Anonymous, LulzSec, and WikiLeaks.



IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 7.39 ⁜ Vol. 11, Issue 4, April 2022

DOI: 10.17148/IJARCCE.2022.114152

8.1 Black Hat Hackers

Black hat hackers are the "bad guys" of the hacking scene. They go out of their way to discover vulnerabilities in computer systems and software to exploit them for financial gain or for more malicious purposes, such as to gain reputation, carry out corporate espionage, or as part of a nation-state hacking campaign. These individuals' actions can inflict serious damage on both computer users and the organizations they work for. They can steal sensitive personal information, compromise computer systems, and alter or take down the functionality of websites and critical networks.

8.2 White Hat Hackers

White hat hackers can be seen as the "good guys" who attempt to prevent the success of black hat hackers through proactive hacking. They use their technical skills to break into systems to assess and test the level of network security, also known as ethical hacking. This helps expose vulnerabilities in systems before black hat hackers can detect and exploit them. The techniques white hat hackers use are similar to or even identical to those of black hat hackers, but these individuals are hired by organizations to test and discover potential holes in their security defenses.

8.3 Grey Hat Hackers

Grey hat hackers sit somewhere between the good and the bad guys. Unlike black hat hackers, they attempt to violate standards and principles but without intending to do harm or gain financially. Their actions are typically carried out for the common good. For example, they may exploit a vulnerability to raise awareness that it exists, but unlike white hat hackers, they do so publicly. This alerts malicious actors to the existence of the vulnerability.

7. CONCLUSION

Viruses have stimulated scientific thinking and ideas. Some ideas can also be exported into medical science. Some viruses can also be put to constructive use (good viruses). Each user must must realise the grave danger posed by viruses. Take steps to prevent infection, and in case of infection, proper and safe ways of dealing with the infection.

8. REFERENCES

A.Coulthard and T.A. Vuori (2002), Computer Viruses : a quantitative analysis Logistics Information Management, Volume 15. Number 5/6. 2002. PP.400- 409, ISSN 0957 – 6053

Ajayshivaa (2007). Symptoms of virus attacks [Online] February 28, 2007. Available from : http://www.astahost.com/info/tiposc-symptoms-virusattack.html. [Accessed: 20th May 2013]

Babak Bashari Rad, Maslin Masrom and Suhaimi Ibrahim (2011), Evolution of Computer Virus Concealment and Anti-Virus Techniques: A Short Survey, IJCSI International Journal of Computer Science Issues, Vol. 8, Issue 1

Essam Al Daoud1, Iqbal H. Jebril and Belal Zaqaibeh (2008), Computer Virus Strategies and Detection Methods, Int. J. Open Problems Compt. Math., Vol. 1, No. 2.

Frederick B. Cohen and Sanjay Mishra (1992) "Experiments on the Impact of Computer Viruses on Modern Computer Networks"

F-Secure Corporation (2001) , "Computer Viruses – from an Annoyance to a Serious Threat". White Paper

Joan C. Hubbard, and Karen A. Forcht (1998), Computer viruses: how companies can protect their systems, Industrial Management & Data Systems, MCB University Press ISSN 0263-5577

Joseph Wen H (1998), Internet computer virus protection policy, Journal of Information Management & Computer Security 6/2 66–71 MCB University Press. ISSN 0968-5227

Kendria (2011). Types of viruses and their effects on your PC [Online] April 7, 2011.Available from http://techgyo.com/index.php/types-viruses-effects-pc. [Accessed: 22th May 2013]