IJRAR.ORG E-ISSN: 2348-1269, P-ISSN: 2349-5138

INTERNATIONAL JOURNAL OF RESEARCH AND ANALYTICAL REVIEWS (IJRAR) | IJRAR.ORG

An International Open Access, Peer-reviewed, Refereed Journal

COMPUTER VIRUS AND ANTIVIRUS

Anusha Srivastava[1], Sanchita Srivastava[2], Swati[3], Abhishek Shahi[4]

[1,2,3]B. Tech Students, Department of Computer Science and Engineering, Buddha Institute of Technology
GIDA Gorakhpur, Uttar Pradesh, India

[4]Asst. Professor, Department of Computer Science and Engineering, Buddha Institute of Technology GIDA Gorakhpur, Uttar Pradesh, India

***Abstract* -** Computer viruses are executable code programs with the unique capacity to replicate themselves in computer systems and spread quickly from one to another. Causing files, documents, and programs to behave abnormally running. Viruses are represented as computer patterns. In computer systems, there are instructional codes that exist over time. Antiviruses are programs that are designed to protect your computer from viruses. Developed to combat the threats posed by viruses such as they defend computer systems from viral attacks by relying significantly on the restrictions that have been added to their databases antivirus software scans the machine using a variety of techniques. Byte patterns suggestive of known viruses to keep up with the times, they must be antivirus software developers who regularly update their products. When new viral strains emerge, they are added to databases. This is a paper about examines the numerous viral types of viruses and antivirus.

INTRODUCTION

As we know, in this 21st century, computers are our basic need. We have a lot of work to do on its network. And to connect two or more networks we have computer networks in many areas or if we say in all over the world (e.g., LAN, MAN, WAN) which connect us from one network to other.

But have we noticed due to this network connection we may also face loss of our many data? If not, then we should pay attention to these small needs of protection. Due to some computer viruses or any threats, we may face our loss of data. So, it's very necessary to prevent them from these viruses. And for its prevention measure, there are many security tools provided which we can use and protect our data.

There is antivirus also provided for its security purpose. There is a set of antivirus packages we can get as per our needs. 'Antivirus' is by its name it is clear that it is used to stop the attack of viruses on the computer and its network.

This research paper is all about computer viruses and their types, their security tools provided, and all about antivirus.

COMPUTER VIRUS DEFINITION

A computer virus is a piece of code that can duplicate itself and usually has negative consequences, such as damaging the system or deleting data.

If we consider the computer as a body and virus as a disease then we can understand it easily. Like a disease, a virus is also made to harm the body or system. The minor difference between them is this disease attack or harm the living body whereas a virus attacks our computer body. It attacks our data and results in data losses.

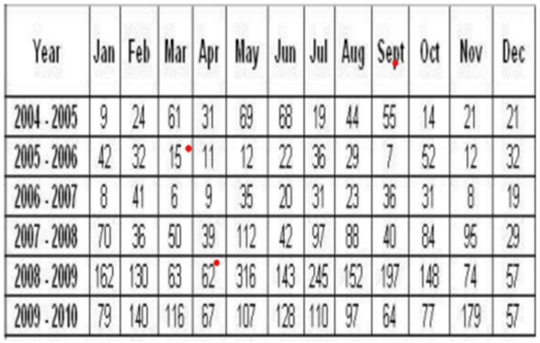
HISTORY OF VIRUS

There are so much to say about its history. Computer virus have been spread from many years ago. Almost every day different types and different version of virus form and spread through internet or its component to computer or our system. They are designed or made to attack on system's information.

There is endless argument about discovery of first virus [16]. In 1970, some people said that first virus had created. But some of them are against this statement and replied that it was not a virus but a malware attack only. The first computer virus, called 'CREEPER SYSTEM' [17] which was released in 1971. It was self- replicating virus made to make improper functioning of computer system. This virus was created by BBN technologies in United states US [17].

Table below shows year wise total number of viruses from 2004 to 2010.

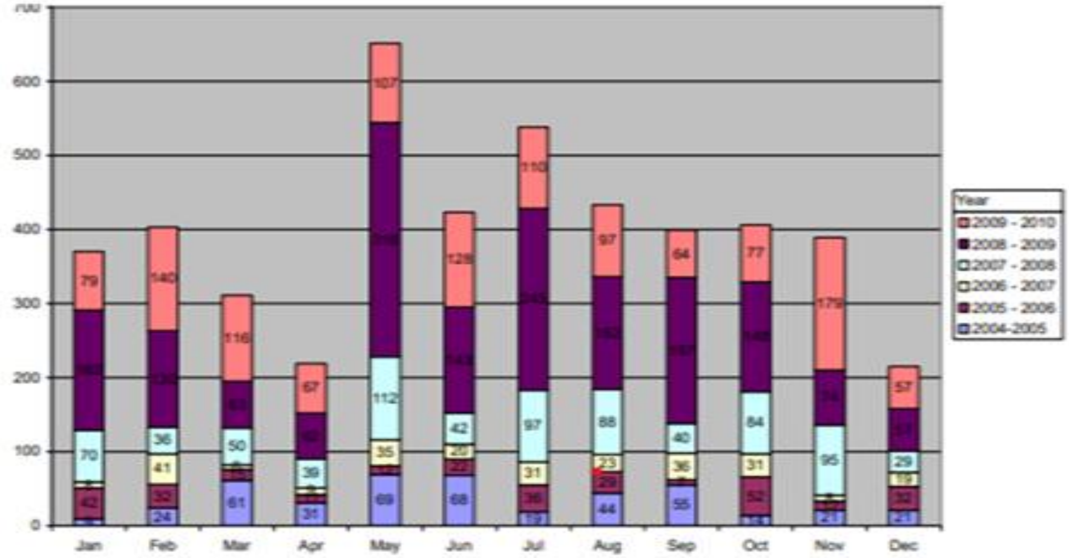
Table 1: year wise total number of viruses [16]



Year	Jan	Feb	Mar	Apr	May	Jun	Jul	Aug	Sept	Oct	Nov	Dec
2004 - 2005	9	24	61	31	69	68	19	44	55	14	21	21
2005 - 2006	42	32	15	11	12	22	36	29	7	52	12	32
2006 - 2007	8	41	6	9	35	20	31	23	36	31	8	19
2007 - 2008	70	36	50	39	112	42	97	88	40	84	95	29
2008 - 2009	162	130	63	62	316	143	245	152	197	148	74	57
2009 - 2010	79	140	116	67	107	128	110	97	64	77	179	57

There is also virus for MS-DOS and the first virus of this was "BRAIN". It was released in 1986. It would overwrite the boot sector on the floppy disk and prevent the computer from booting [17]. It was written by two brothers from country name 'Pakistan'.

Chart 1:Year wise total number of total viruses [16]



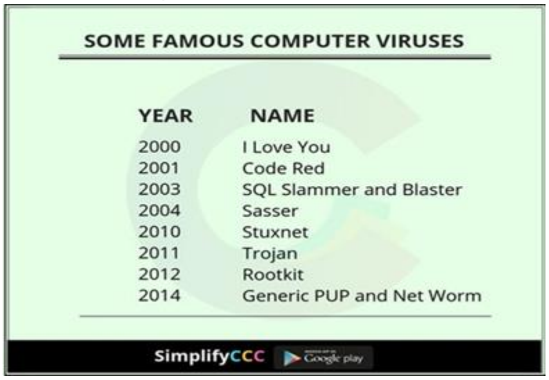
In 1988, there was another virus name as 'The Morris' made or written by Robbert Morris. He had made it for measuring size of internet but due to some mistake in its programming or coding it infects around 1000 system in one hour. As an effect of it, it started interfering with the system's normal function. Since then, many viruses have been introduced and trend is growing exponentially every year [17].

NAMES OF VIRUSES

There are some popular names of the virus as follows:

- iloveyou
- Code red
- Sasser
- Zeus
- mocmex
- Cryptolocker
- Daprosy worm

Figure 1: Name of viruses



SOME FAMOUS COMPUTER VIRUSES

YEAR	NAME
2000	I Love You
2001	Code Red
2003	SQL Slammer and Blaster
2004	Sasser
2010	Stuxnet
2011	Trojan
2012	Rootkit
2014	Generic PUP and Net Worm

SimplifyCCC
Google play

Let’s see each in detail.

1) iloveyou-

- This virus was discovered in May 2000.
- It arrives by email or is entered into the system with the notation "I adore you." It may also be accompanied with a file named "LOVE-LETTER-FOR-YOU.txt.VBS" [11].

2) Code red-

- This virus was discovered in July 2001.
- It is used to attack the system by worms by executing arbitrary code.
- Also attack by machine with worms [11].

3) Sasser-

- This virus was discovered in April 2004.
- It attacks the system by its IP address.
- It chooses any IP address in its range and attacks on it particularly by connecting it by TCP.

4) Zeus-

- It was discovered in July 2007.
- It is formed by downloading something through the drive.

5) mocmex-

- This virus was discovered in February 2008.
- It is a virus that mainly attacks frames like a photo frame.

6) Cryptolocker-

- This virus was discovered in September 2013.
- It is a combination of crypto+locker.

· Here, crypto means encrypting and decrypting and lock means encrypting the file.
· So, it’s mainly attacked by encrypting the user’s disk.

7) Daprosy worm-

· This virus was discovered in July 2009.
· It focuses on stealing passwords and form like this.
· It’s mainly focused on stealing an online game password

PROTECTION OF SYSTEM FROM COMPUTER VIRUS

- **USE A FIREWALL-**

We should always use a firewall to protect our system from viruses. The firewall worked as a security guard to the system which do not allow any virus or harmful file to come into our system.

- **UP-TO-DATE SOFTWARE-**

We should keep in mind to on automatic update. It makes sure to update all your software, your windows, etc to be updated for its security purpose**.**

- **USE ANTIVIRUS-**

We should use the right antivirus for different viruses on our system. For e.g., on the window, there is a window security antivirus which is already installed on our window.

- **UNSUSPICIOUS LINK-**

Make sure not to open any link which is not known to you to protect the system from viruses. These links can contain a virus or harmful files in it.

- **TRUSTED SOURCE-**

Avoid using untrusted sources. If you are downloading something like a movie or anything then make sure to download it from a trusted link or source.

- **EXTERNAL DEVICES-**

Avoid using an external device that is not yours. It may contain a virus or malware in it. It can harm our system. Use any USB cable or any external device which is owned to you or to any trusted user**.**

- **CHOOSE PASSWORD-**

Choose your password carefully. It should be strong and can't be easily guessed by anyone.[4]

CLASSIFICATION

People who are good for nothing create viruses. But sometimes when someone wants to prove his or her point, they create viruses. For example, if a computer expert wants to show you that a certain process will work or that a certain network can be breached, or that certain antivirus software is productive. So, these types of reasons are used to prove someone's point by actions rather than theories. there are many types of computer viruses available at this time .

Viruses can be classified on the basis of:

- On the basis of types of infected objects viruses can be of three types:

when these type of computer viruses enters a computer, it duplicates themselves by modifying other computer programs and inserting their own code. In this case, if the duplication completes, the area of code which is duplicated is called an infected area.

1. FILE VIRUS

file viruses are also called file infectors. they generally copy their own code on the executable file and duplicate it in the computer system. This malware is used to infect the executable file and damage them permanently so that it can't be used in the future.

2. BOOT VIRUS

Boot viruses are also called boot infectors. It infects the boot sector of computers.

During system boot, boot viruses are loaded into the main memory and destroy data stored in the hard disk. The BRAIN boot sector virus was the first PC virus that began infecting floppy disks in 1986. two brothers named Basit and Amjad Farooq Alvi have created this virus.

3. MACRO VIRUS

Macro viruses are written in a macro language i.e., a programming language that is embedded within a software application. these viruses are sets of instructions that can be triggered by a command. These viruses are associated with application software like word and excel. when you open the infected document the macro virus is loaded into the main memory and destroys the data stored in the hard disk. The first macro virus was written for Microsoft word and was discovered in august 1995. There are hundreds and thousands of macro viruses available these days some common examples are- WM.concept, Melissa, and Nimda.

- On the basis of Payload viruses can be of three types:

A payload refers to the part of transmitted data that executes a malicious activity. Viruses with more powerful payloads tend to be more harmful.

1. ROOTKIT

A rootkit is a collection of tools for retaining root access to a computer system. It is a collection of files designed to hide from normal detection by hiding processes, ports, files, etc. The first rootkit for malicious NT operating system discovered in 1999, is a type of trojan known as NTRootkit. This rootkit is created by Greg Hoglund . there are various types of rootkits available: -

- Binary rootkit
- Kernel rootkit
- System call rootkit
- Library rootkit
- Virtual machine rootkit
- Database rootkit
- Runtime Kernel patches
- Userspace
- Kernel Space

2. SPYWARE

Malicious Software that is installed, without you knowing or without asking your permission is Spyware. In 1999 when a famous game known as Elf Bowling came in which tracking software are attached then the first spyware was introduced to internet users. they can be of many forms:

- Adware – they monitor all the activities that you do on the browser so that they can show you only those advertisements in which you are interested.
- Trojans – they are impersonating as a permissible file so that after downloading it can access your data.
- Internet tracking – monitors and follow all the web activities such as your downloads, what you search on the internet, and all your browsing history.
- System monitors – they can know what you are typing on your keyboard and everything you do on your personal computer.

3. BACKDOOR

The methods through which we can access any computer program and for these means' security mechanism is nothing i.e., they can penetrate the security mechanism. Backdoor tactics are what they're called. Mostly Backdoors are used by programmers so that they can get access to the program for various fixing causes. The Backdoor is also called the six-finger plan, this is the first time conceived by Marvin Latimer and Nakomis Dedmon.

✚ On the basis of Way of penetration viruses can be of two types:

1. **TROJAN HORSE**

The main intention of a trojan horse is to divert the user. It actually works completely opposite to its function. Firstly, it appears to be not harmless but can be destructive. The first trojan horse virus in a computer is developed in 1975 by john walker and is called ANIMAL .

2. **EXPLOIT**

Exploits are generated to attack software vulnerabilities. Through various methods, users are attracted to execute exploits. And the whole control of the system is accessed by the attacker by dropping malware. The first Exploit was detected in 1970 and called the creeper virus . The Exploits can arrive through various means like: -

- May attached to an email message
- Unknown website that can be harmful
- Various social media platforms
- May directly attaches to weak server

✚ On the basis of Way of penetration viruses can be of three types:

These infections hide in computer systems and are difficult to detect by antivirus software.

1. POLYMORPHIC

A polymorphic virus is a virus that changes its form by changing its own code each time it replicates itself. Due to its replication, it is not easily detectable. This virus is always tried to hide from antiviruses by encrypting itself. The encrypting process is called a mutation. The first Polymorphic virus was developed by Mark Washburn in 1990. The name of the first virus is 1260 . The metamorphic virus is the hardest virus to detect because it changes its internal structure.

2. **STEALTH VIRUS**

These types of viruses not only hide the virus signature but also hide the damage they do. These viruses attack operating system processes and bind to files, disk partitions, and boot sectors so that they can't be detected. The first stealth virus is known as Brain which is used to aim the IBM PCs and infected many storages disk .

3. **ENCRYPTED VIRUS**

These viruses are the deadliest viruses. These viruses enter your system and start encrypting your files and documents. When your data is encrypted, you can't access them unless you have the key. Its main function is to steal all the important stuff of yours and all the computer attached to your system in the network. Cascade was the first encrypted viruses of computer systems that appeared in 1984

PROGRAMMING LANGUAGES USED TO WRITE VIRUS

Programming languages used by programmers to communicate with computer system. The basic building unit of today's technology is programming languages. All the things we do on internet are basically done by programming languages weather it is good or bad.

With the help of programming language, we give the computer a set of instruction so that the computer can follow the rules and make our work done. In these days various programming languages are available and they have their own set of rules, instructions and syntax.

There are two types of languages are available on basic level:

- Low level language:

These languages are dependent on machine, means there are only 0's and 1's in this language type. This language does not need to be translated by compiler or interpreter so the processing of this language is extremely fast.

There are two types of low-level language Machine language and assembly language.

Machine language are easy to understand by the computer because they are in machine code while assembly language needs assembler to make them understandable to computer.

- High level language:

High language is easily understandable by the user. This language is used to make user friendly environment. The language we directly write on the system like English is high level language. High level language can't be understood by computer directly so we use compiler or interpreter to translate them so that they can be easily understandable to computer.

The most popular programming languages are:

- Python
- C
- Java
- C++
- C#
- R
- Java Script
- Go
- Swift
- Ruby
- BASIC
- COBOL
- FORTRAN
- Ada
- Pascal

The programming language that hackers prefer are according to their need and depend on what type of work they want to be done. All the malwares are written in C because it is a general-purpose programming language. The C language is used for various type of computing environment. An exploit uses JS, ActionScript, VB script and Java for using computer vulnerability and using it for their advantages. The exploit basically comes In SQL attacks or writing a malicious code into a website. Python is used for remote attack because it is in compare to the C language. So, there is no need of interpreter to change the source code, python can be directly used. C# and C++ languages are used to develop high level viruses. This type of viruses take time to be developed and are more complex. For mobile malwares are created using Java and a little more use of C and C++.

Mostly, virus developer is using these four languages these days—Go, DLang, Nim and Rust—to either recycle viruses or as powerful approach to not give away their wicked code from safeguard equipment's, for the time being escaping scrutiny attempt by researchers. That's stated in a fresh report proclaimed by BlackBerry's Research & Intelligence division [15].

IMPLEMENTATION OF VIRUSE ANALYSIS

Virus analysis process can be described as the process by which we study the conduct and factor of a virus.

When you perform a virus analysis, do not panic by the information of the virus. You must set a goal for your analysis. Ask yourself why are you doing this analysis? Or what is the main mechanism of the virus? When you know which type of virus is affection your system you can find the cure for it.

After setting your goal do analysis on your virus type. Basically, there are two types of malware analysis:

1. Static analysis
2. Dynamic analysis

- **Static analysis:**

Static analysis is also known as code analysis. Code analysis is done by inspecting physical code of the virus and concluding what it is really doing.

- **Dynamic analysis:**

Dynamic analysis is also known as Behavioural analysis. Behavioural analysis determines what is the conduct of the virus after execution i.e., what it does, whom it talk, what it writes, etc.

FIGURE: Malware Analysis Tools [22].

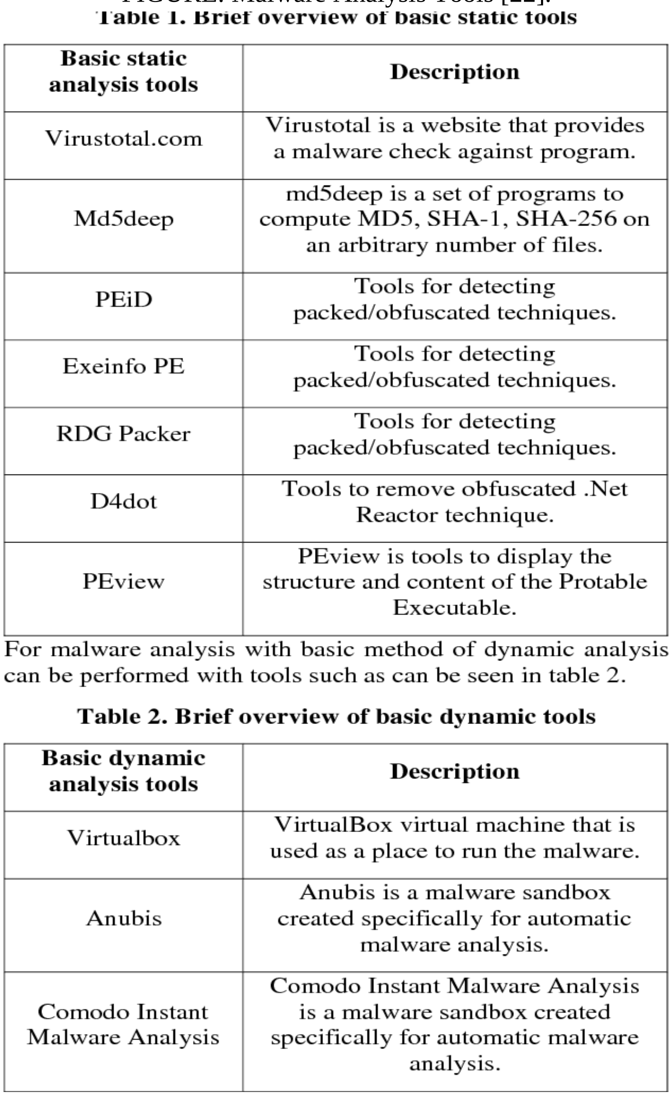


Table 1. Brief overview of basic static tools

Basic static analysis tools	Description
Virustotal.com	Virustotal is a website that provides a malware check against program.
Md5deep	md5deep is a set of programs to compute MD5, SHA-1, SHA-256 on an arbitrary number of files.
PEiD	Tools for detecting packed/obfuscated techniques.
Exeinfo PE	Tools for detecting packed/obfuscated techniques.
RDG Packer	Tools for detecting packed/obfuscated techniques.
D4dot	Tools to remove obfuscated .Net Reactor technique.
PEview	PEview is tools to display the structure and content of the Protable Executable.

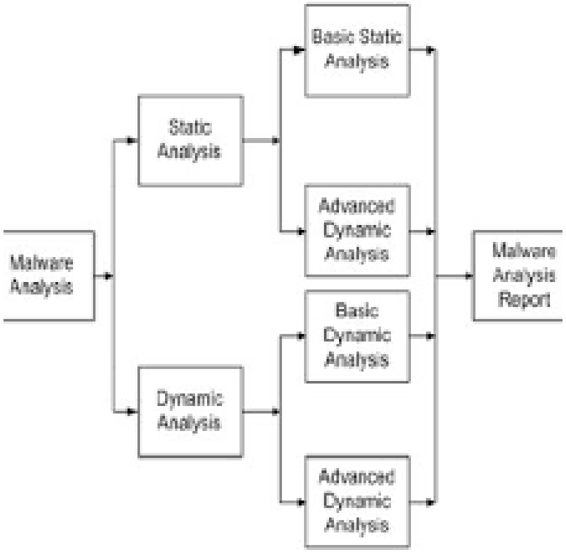
For malware analysis with basic method of dynamic analysis can be performed with tools such as can be seen in table 2.

Table 2. Brief overview of basic dynamic tools

Basic dynamic analysis tools	Description
Virtualbox	VirtualBox virtual machine that is used as a place to run the malware.
Anubis	Anubis is a malware sandbox created specifically for automatic malware analysis.
Comodo Instant Malware Analysis	Comodo Instant Malware Analysis is a malware sandbox created specifically for automatic malware analysis.

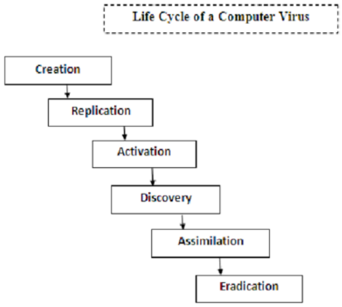
Bot the analysis must accomplish to get the complete picture of how the virus is behaving and operating. By sophisticated by the operation of the virus we can easily understand its function and can be aware of what it going to do to the vulnerabilities of our system. Then, we can accommodate a protection against the threat [12].

FIGURE: Malware analysis [22]



LIFE CYCLE OF THE VIRUS

Figure 2: Lifecycle of virus [5]



It is a step wherein virus created with the aid of using the individuals who need to make harm in anyone's device.

- **REPLICATION:**

It is a step wherein many shapes of virus shape. Viruses divide themselves in lots of paperwork so that to assault on many structures at an identical time.

- **ACTIVATION:**

When a virus comes into the device then it turns on itself.

- **DISCOVERY:**

It is shaped whilst the virus finds out itself or whilst it has become a threat. It can /might also additionally come at the least one time in a year. It does now no longer find out each time.

- **ASSIMILATION:**

It is a 2d remaining level of virus. It got here whilst antivirus stumbles on the virus to kill it or eliminate it from our device.

- **ERADICATION:**

It is a remaining level of virus wherein it eliminates or we can say wherein it's miles dead. It may be are available at this level whilst person locates proper software program to put in into device to kill it for completely.

BEHAVIOUR OF VIRUS

For infecting any device any virus wishes time. They don't assault immediately "VIRUS WRITERS HAVE TO BALANCE HOW AND WHEN THEIR VIRUSES INFECT AGAINST THE POSSIBILITY OF BEING DETECTED. AS A RESULT, THE BEHAVIOR OF AN INFECTION CAN BE IMMEDIATE OR DELAYED"

Viruses have numerous extraordinary degrees of infection. They infect any pc in degrees. The first level is referred to as Infection level and the second level is referred to as assault level.

- **INFECTION STAGE-**

With each execution of a plague, your software will infect. But it isn't flawlessly comprehensible whilst it will likely be carried out. The virus may be carried out on a cause or input your pc and begin off evolved executing. If you observed you're executing software and there's no virus in it, if its miles going for walks smoothly, it's miles viable that the virus will execute a while later or on a specific cause. Many viruses disguise for your reminiscence after coming into your computer and anticipate a sure occasion or a record or report to open so one can begin their execution. You'll in no way realize what the one's occasions, those kinds of viruses are very tough to analyze.

"It's critical to word that WORMS frequently take the alternative method and unfold as speedy as viable. While this makes their detection truly sure, it's also having the impact of bringing down networks and denying access; one of the desires of many worms" [10].

- **ATTACK STAGE-**

Many viruses do numerous matters which aren't excellent for you and your device. They thieve your records, make modifications for your records, or gradually down your reminiscence. They could make seem like a few messages to your pc screen. Sometimes you can't open a few records or reports due to the fact they may be encrypted with the aid of using the virus and also you want the key to decrypt it. Still despite everything of this sort of occasion in case you assume that your Pc is attacked with the aid of using a plague then the solution is no. Every virus has a few impacts due to the fact they have a few insects in it which reason those kinds of occasions arise to your Pc.

Viruses try and disguise their presence; they don't need to be detected. So, for the assault section to begin virus can take months, years, a long time, and a few viruses duoviruses assault your device they simply input your device and begins off evolved replicating themselves. That doesn't suggest that if a plague isn't doing something it is a great virus, that virus continues to be making modifications for your PC without taking your permission this is nevertheless taking your reminiscence area so it's miles nevertheless now no longer excellent in your computer.

DENIAL OF SERVICE ATTACK

It is also known as DOS. A Denial-Of- Service (DOS) attack is an attack meant to shut down machine or network, making it inaccessible to its intended users [18]. This attack attacks the machine by trafficking the target or by sending information that triggers a crash. It's not focus on losing data of system but it focuses on user's major loss of time and their money. It mainly targets on high profile web servers. It includes attacks on banking sector, trade sector, media company or any government sector web server.

There are two method includes: flooding or crashing service.

FLOODING SERVICE: It includes flood attack due to which system receives unaffordable amount of traffic which makes the system work slowly and make it stop eventually.

There are many floods attack in which some of popular flood attacks are:

➢ Buffer overflow attack:

- It is most common Denial of Service attack.
- Its main focus it to send lot of traffic to targeted network and makes the system work slow.

➢ ICMP Flooding:

- It is also known as smurf attack.
- It is used by sending packets of spoofed and misconfiguring network devices.
- It's not focus on only one device but on every device of that targeted network.

TYPES OF DOS:

There are different types of DOS (Denial of service) attack in computer world. The most important type of DOS are as follows:

➢ Syn Flooding attack

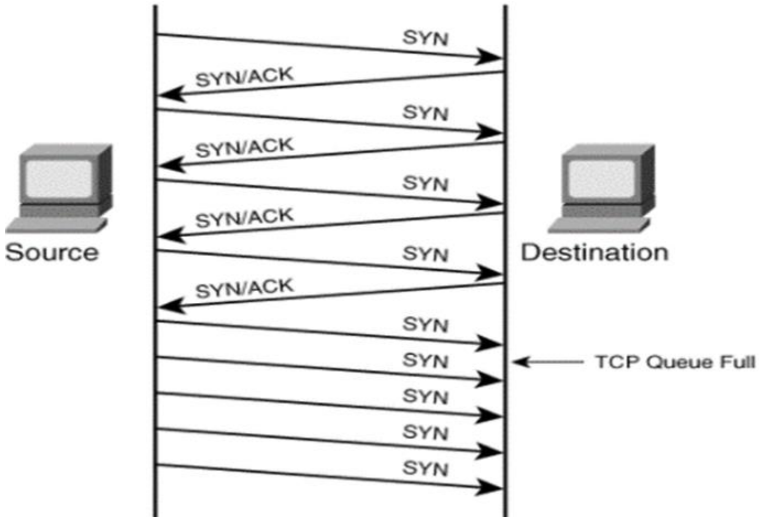
➢ Application layer attack

➢ DDOS attack

Syn flooding ATTACK:

1) As by its name, it is clear that here we are using flooding service concept.
2) In this type of attack, attacker carry multiple zombies with him and flood the target with more than one SYN packets.
3) As a result of it, target will start working slowly and its performance is reduced.
4) It sends a request to connect to server but never completes the handshake [19].

Figure 1:Syn flooding



<u>Application layer attack:</u>

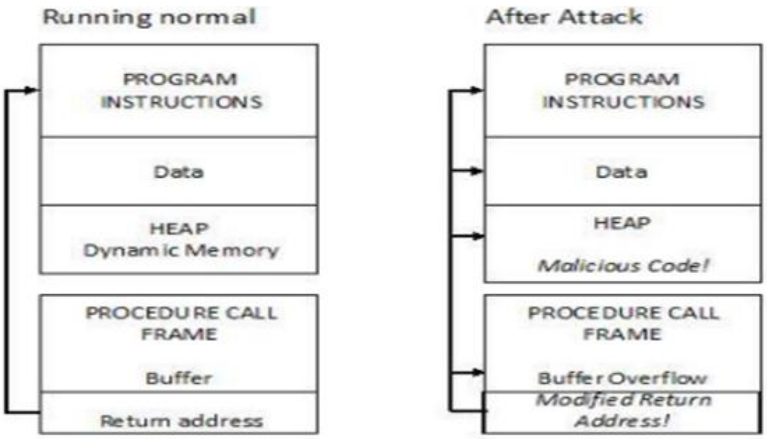
1) In this type of attack, its attack caused due to error in application.

2) Here, attacker takes good advantage of programming error in application.

3) This attack is caused by sending number of application request at a time to target application so that it gets confused in between them and could not perform service of valid client.

4) It comes under buffer overflow attack as when memory allocated to variable is smaller than the requested one then it may lead to memory leakage or crashing the entire application [19].

Figure 2: Application Layer Attack[19]



Attacker plants code that overflows buffer and corrupts the return address. Instead of returning to the appropriate calling procedure, the modified return address returns control to malicius code, located elsewhere in process memory.

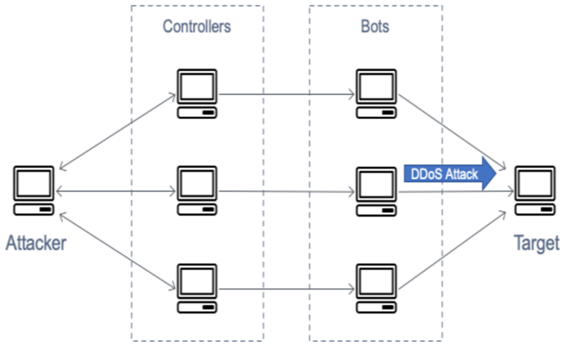
<u>DDOS attack:</u>

1) DDOS attack is abbreviated as Distributed Denial of Service.

2) It occurs when multiple system orchestrates a synchronized DOS attack to a single target [18].

3) It is different from denial-of-service attack.

Figure 3: DDOS Attack [20]



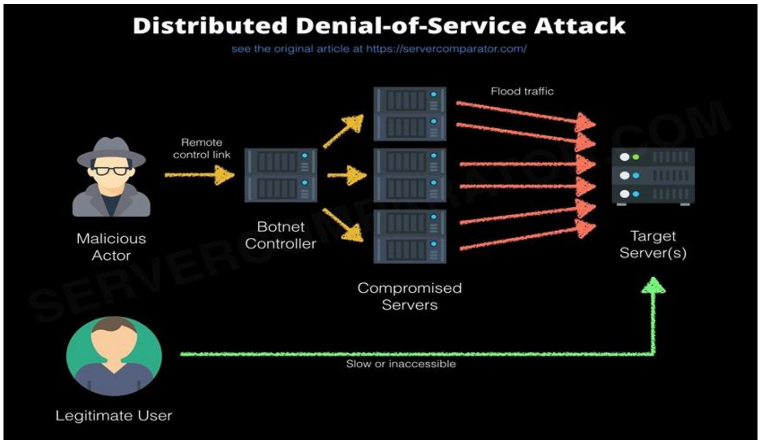
6) The main difference between them is Denial of Service attack target only one location but Distributed Denial of service attack targets more than location at a single time.

7) It gives more profit to attacker than DOS.

8) The main advantage he can get is it is difficult to identify attacker identity as it is comprised behind many systems.

9) It is very difficult to shut down more than one system at a single time which also works as a advantage to attacker.

Figure 4: DDOS Attack [21]



ANTIVIRUS SOFTWARE

Antivirus Software aims to prevent access to computer systems by unwanted computer malware. Viruses, worms, or trojan horses can be used by criminals or mischievous people (called 'hackers'). They can be used to steal information or damaged system files. If no antivirus software is installed on a computer, hackers may be able to access the information in the computer [1].

ANTIVIRUS FEATURES

Antivirus software has been one of the most important parts of the IT industry since consumers and businesses first began linking their computers to the internet decades ago. It's grown so common that many people mistakenly believe that every antivirus software provides the same amount of security and capabilities, and they don't pay attention to the product they're using. The antivirus software you use can have a big impact on your capacity to successfully defend yourself against malware and threats. There are a few key aspects to look for in an antivirus solution before deploying it throughout your entire system

Scanning in Real Time

While all antivirus software is designed to identify malware, not all antivirus software detects malware in the same way. Ineffective programmes force you to do a manual scan to see if any of your systems have been compromised, whereas the finest software has dynamic scanning tools that check your computer for harmful entities on a regular basis. It's far easier for something to penetrate your computer and start inflicting damage before you ever notice it if you don't have this function.

Updates are made automatically.

Updates are essential for all types of software, but they are especially important for antivirus. Antivirus software requires periodic upgrades to track and control new threats that didn't exist when it was first installed since new varieties of malware are continually being produced. If you have to manually install updates, you risk missing out on critical new protections and exposing your system to infection, so make sure your antivirus software can do so automatically and frequently.

Multiple Apps Protection

Threats can be found in a wide range of apps and services that you use on a daily basis. Harmful software can enter your system through a multitude of channels, including email clients, instant message services, and, of course, web browsers. Antivirus software must defend several vulnerable apps from potential threats; otherwise, your hardware will be at risk.

Auto-Clean

Why wouldn't antivirus software erase dangerous software on the spot if it finds it right away? Unfortunately, some solutions just quarantine malware after it is detected, waiting for the user to log on and manually erase it. Because there's no reason to keep potentially harmful software on your computer, look for a tool that uses an auto-clean feature to remove viruses

Defends Against Malware of All Kind

There are many various varieties of malware that might affect your computer, including trojans, bots, spyware, viruses, and so on, and antivirus systems are occasionally built to only target a certain type of software. It's preferable to use a tool that can identify all or almost all of the numerous forms that malware can take.[23]

What Antivirus Features Should You Prioritize?

1) Simple to Operate

Both end users and administrators must be able to use the solution. Admins generally have multiple programs to administer, so they don't have a lot of time to learn new solutions. As a result, it's critical that the product's usage instructions are clear. Furthermore, an effective antivirus system should place a premium on granularity above end-user visibility. The majority of the time, a good antivirus solution should be completely invisible to the end-user, only sending notifications when it detects a critical or potentially serious occurrence that they should be aware of. If a website is restricted due to an HTTP connection, for example, the user should be notified, but not inundated with messages. If something is blocked, it must be apparent why it is blocked, and you must be able to disable notifications for insignificant operations like updates, quick scans, firewalls, and so on. When a user receives a notification, you want them to pay attention to it instead of dismissing it. When it comes to the ever-present problem of human error, a poor user interface can increase the likelihood of errors and compromise the computer's security. It may even discourage people from using the antivirus program entirely. A decent antivirus solution should have a simplified design that allows the user to complete their daily work duties without losing productivity.

2) Recognize and Respond to Polymorphous Attacks

Polymorphic malware is a type of malware that can evolve and change its features in order to evade detection. Viruses, bots, worms, trojans, and keyloggers that actively modify their identifying traits to elude normal detection approaches fall into this category. The malware continues to infect devices and spread even after its characteristics—such as file names and types of encryption keys—change. This prevents some antivirus solutions from immediately recognizing new file names as malicious, so by the time they are noted and added to the database, the malware could have already changed again. Polymorphic code makes it difficult for security solutions to recognize the malware’s new state after it replicates, due to how frequently it changes itself. Even after it has been repelled once, new iterations of the virus could potentially sneak past your defenses, which can no longer recognize it. A comprehensive antivirus solution protects against this in two ways; heuristic scanning and behavior-based detection. With heuristic scanning, rather than attempting to find an exact match to an already established threat, the goal is to scan for certain crucial components the threats could share, thereby boosting the opportunity to detect and prevent a new variation of the virus. And behavior-based detection serves the function of analyzing the virus’s behavior instead of simply observing its actual code.

3) Automatic Updates

For all forms of software, updates are a necessity. However, this is particularly true when it comes to antivirus solutions since cybercriminals are constantly adapting and creating new, innovative forms of malware. Antivirus software needs to be equally as adaptable, with frequent updates which serve to track and contain new threats which may not have even existed when it was initially installed. Automatic updates are the easiest and most reliable way to keep on top of the most recent threats. If users have to manually install updates, you might find that important new protections are missed, leading to an increased risk of exposing your system to infection.

4) Real-Time Scanning

This is an incredibly important feature in any antivirus product. While all antivirus software is designed specifically to detect the presence of malware, they don't all do this in the same way. Less effective antivirus solutions require you to run a manual scan in order to determine if any systems have been affected, which means you will not find an infected file until after it has already been downloaded, and when you next choose to manually run a scan. This means the damage could have already been done by the time you realize something is wrong. Most of your users will be focused on doing their day-to-day roles rather than wanting to manage their device security, so it's important that scanning is automated and performed in real-time. The best antivirus solutions avoid this problem with dynamic scanning features which automatically and regularly check your computer for any sign of malicious entities. This useful feature makes it easier to avoid having something malicious infiltrate your computer and have enough time to cause serious damage.[24]

5) Backups

This is a feature that a lot of antivirus solutions offer, but not all of them. The benefits of backups are clear: any organization that has experienced a cyberattack or serious data loss would be in a much better position if they could turn to backups without having to think twice. For instance, in the case of a ransomware attack where vital files, documents, networks, or servers are targeted and left encrypted and inaccessible—to learn more about this specific malware issue, read our article on the subject—it can be crippling for business productivity to have no backups in place to keep things moving along while the issue is resolved, which can lead to additional pressure to pay the ransom. A good, reliable antivirus software solution enlists this essential feature, providing peace of mind alongside the ability to restore lost data quickly. Considering how useful this feature can be, it is a good idea to ensure whatever antivirus solution you might consider comes with it.

ANTIVIRUS FUNDAMENTALS: Viruses, signatures, disinfection

We talk and talk (and talk) about how to behave — and even how to survive — in the digital world. And we hope it's not in vain, that our readers learn from us and then teach their friends and relatives. It's really important.

But we sometimes take for granted a common knowledge of some specific terms and expressions. So today we're going back to basics to tackle three fundamentals of antivirus.

1. Signatures

Antivirus databases contain what are called signatures, both in common usage and in writing. In reality, classic signatures have not been in use for about 20 years.

From the very beginning, in the 1980s, signatures as a concept were not clearly defined. Even now, they don't have a devoted Wikipedia page, and the entry on malware uses the term without defining signatures, as if were such common knowledge as to go without explanation.

So: Let's define signatures at last! A virus signature is a continuous sequence of bytes that is common for a certain malware sample. That means it's contained within the malware or the infected file and not in unaffected files.

Antivirus fundamentals: Viruses, signatures, disinfection

A characteristic sequence of bytes

Nowadays, signatures are far from sufficient to detect malicious files. Malware creators obfuscate, using a variety of techniques to cover their tracks. That's why modern antivirus products must use more advanced detection methods. Antivirus databases still contain signatures (they account for more than half of all database entries), but they include more sophisticated entries as well.

As a matter of habit, everyone still calls such entries "signatures." There's no harm in that, as long as we remember that the term is shorthand for a gamut of techniques that make up a much more robust arsenal.

Ideally, we'd stop using the word signature to refer to any entry in the antivirus database, but it's so commonly used — and a more accurate term doesn't yet exist — so the practice persists.

An antivirus database entry is just that: one entry. The technology behind it could be either a classic signature or something super-sophisticated, innovative, and targeting the most advanced malware.

2. Viruses

As you might have noticed, our analysts avoid using the term virus and prefer malware, threat, and so on. The reason is that a virus is a specific type of malware that exhibits a specific behavior: It infects clean files. Between themselves, analysts refer to a virus as an infector. Infectors enjoy a unique status in the lab. First, they are difficult to detect — at a glance, an infected file seems clean. Second, infectors require special treatment: almost all of them need specific detection and disinfection procedures. That is why infectors are handled by experts who specialize in this field.[25]

Antivirus fundamentals: Viruses, signatures, disinfection

Malware, classified

So, to avoid confusion when talking about threats in general, analysts use umbrella terms such as "malicious program" and "malware."

Here are a couple of other classifications that may come in handy. A worm is a type of malware that can replicate itself and break out of the device it initially infected to infect others. And malware, technically speaking, does not include adware (intrusive advertising software) or riskware (legitimate software that can inflict harm on a system if installed by malefactors).[25]

3. Disinfection

Lately, I've been seeing a lot of what I hope is not a common misperception: that antivirus can only scan and detect malware, but then a user needs to download a special utility to remove the malware. In fact, special utilities do exist for certain types of malware: for example, decryptors for files affected by ransomware. But antivirus can cope on its own — and at times it's the better option, provided access to system drivers and other technologies that cannot fit into a utility.

So, how does malware removal work? In a tiny percentage of cases, a machine picks up an infector (typically before antivirus is installed; infectors seldom slip through an antivirus's defenses), the infector acts on some files, and then the antivirus goes through any infected files and removes the malicious code, restoring them to their original state. The same procedure is implemented when you need to decrypt files encrypted by ransomware, commonly detected as Trojan-Ransom.

As for the rest — the vast majority, perhaps 99% of cases — the malware is caught before it can infect any files, the process consists of simply deleting the malware. If no files were damaged, there's no need to restore anything.

Antivirus fundamentals: Viruses, signatures, disinfection

In the majority of cases, it's enough to delete the malicious file

There is one exception here, though: If the malware is not an infector – for example, if it is ransomware – and is already active in the system, the antivirus switches to disinfection mode to make sure the threat is gone for good and won't come back. You can learn more about the process here.

That exception usually happens for one of two reasons:

- The antivirus was installed onto an already infected computer. You know, the usual wrong sequence — first get infected, than decide it's time to do something about protection.

- The antivirus marked something "suspicious" rather than "malicious" and started to closely monitor its activities. As soon as the malware becomes clearly malicious, the antivirus rolls back all malicious activities (noted during that period of monitoring). For example, the antivirus could restore encrypted files from instant backup copies if the PC was attacked by ransomware or an infector.[25]

WHAT IS A SIGNATURE?

In computer security terminology, a signature is a typical footprint or pattern associated with a malicious attack on a computer network or system. This pattern can be a series of bytes in the file (byte sequence) in network traffic. It can also take the form of unauthorized software execution, unauthorized network access, unauthorized directory access, or anomalies in the use of network privileges.[26]

WHAT IS SIGNATURE DETECTION?

Signature-based detection is one of the most common techniques used to address software threats levelled at your computer. These threats include viruses, malware, worms, Trojans, and more. Your computer must be protected from an overwhelmingly large volume of dangers. Achieving this protection is hugely dependent on a well-crafted, advanced, signature-based detection being at the helm of affairs.

This type of detection involves your antivirus having a predefined repository of static signatures (fingerprints) that represent known network threats. These threats are different from one another because of their unique coding.[26]

When the antivirus scanner kicks into action, it begins creating the appropriate signatures for each file and starts comparing them with the known signatures in its repository. It keeps monitoring and searching network traffic for signature matches. If a match is found, this file is categorized as a 'threat' and the file is blocked from taking any further action.[26]

WHAT MAKES SIGNATURE-BASED DETECTION SO POPULAR?

Identifying malicious threats and adding their signatures to a repository is the primary technique used by antivirus products. Signature-based detection is also the critical pillar of security technologies such as AVs, IDS, IPS, firewall, and others.

Its popularity is buttressed by its strength. It's been used since a very long time, since the first antivirus solutions appeared on the scene. So, there is a degree of consistency of results and demonstrable success associated with it. The approach isn't very complex, is fast, easy to run and manage. And what's more, it has chalked up a history of protecting computers from the fairly older but potent threats.[26]

Integral component of a layered approach to security

There is absolutely no doubt signature-based detection is a critical component of your computer's security arsenal, but the threat landscape you see in front of you isn't static: It is evolving rapidly. The threats are becoming more sophisticated, and every day, stealthier attack techniques are entering the fray.

There is a need for a more layered security approach, where signature-based IDS is used in conjunction with other security methods. These include behavior-based detection, AI threat detection, advanced malware scanning, and remote security management. Sophos Home brings next-gen enterprise level security to your PCs and Macs at home. Sophos Home protects from threats of all kinds, whether signature-based, signature-less, or any other online threat. Download it today to see it for yourself.[26]

What Is an Intrusion Detection System (IDS)?

An intrusion detection system, IDS for short, monitors network and system traffic for any suspicious activity. Once any potential threats have been identified, intrusion detection software sends notifications to alert you to them. The latest IDS software will proactively analyze and identify patterns indicative of a range of cyberattack types. An effective solution should be able to discover any threats before they fully infiltrate the system.

Firewalls and anti-malware programs are just one small part of a comprehensive approach to security. When a network grows, and unknown or new devices regularly jump in and out, you need intrusion detection software. This software should be capturing snapshots of your whole system, using knowledge of potential intrusions to proactively prevent them. Intrusion detection system software is usually combined with components designed to protect information systems as part of a wider security solution. A full-fledged security solution will also feature authorization and authentication access control measures as part of its defense against intrusion.

While this is the basic function and purpose of intrusion detection software, not all programs are created equal. Some let you implement rules, which the program then uses to inform and execute certain actions and tasks, while others do not. Open-source IDS options are also available, which can differ significantly from closed source software, so it's important to understand the nuances of an open-source network intrusion detection system before choosing it.

The latest IDS software programs are likely to include specialist and advanced features, so it's worth considering how useful these more sophisticated components would be to your business. After all, it maynot be cost-effective for an organization with minimal network intrusion detection requirements to choose the most advanced and latest IDS software.[27]

Before getting into my favorite intrusion detection software, I'll run through the types of IDS (network-based and host-based), the types of detection methodologies (signature-based and anomaly-based), the challenges of managing intrusion detection system software, and using an IPS to defend your network.

TYPES OF IDS

An intrusion detection system comes in one of two types: a host-based intrusion detection system (HIDS) or a network-based intrusion detection system (NIDS). To put it simply, a HIDS system examines the events on a computer connected to your network, instead of examining traffic passing through the system. As its name suggests, it's based around the host. A NIDS, on the other hand, examines the network traffic.

* Network-Based Intrusion Detection System (NIDS)

As a system that examines and analyzes network traffic, a network-based intrusion detection system must feature a packet sniffer, which gathers network traffic, as standard. Though NIDSs can vary, they typicallyinclude a rule-based analysis engine, which can be customized with your own rules. In some cases, NIDSs have a user community producing rules you can import directly, to save you time. It may take some time to get familiar with the rule syntax of your chosen NIDS and being able to import from the user community can make the initial NIDS implementation feel like less of a steep learning curve.

NIDS rules also facilitate selective data capture. This is necessary because if you were to feed all your traffic into files or run it through a dashboard, data analysis would be pretty much impossible. So, if you have a rule designed to flag up suspicious HTTP traffic, your NIDS will filter out irrelevant data and only store HTTP packets with specific characteristics. This keeps the system from being overwhelmed.

A NIDS program usually gets installed on a specific piece of equipment. The high-end, enterprise-grade solutions typically come in the form of a network kit with the program built in. A NIDS requires a sensor module for picking up traffic, but you don't necessarily need to pay out for expensive hardware. You could load a sensor module onto a LAN analyzer or specify a device to run the task. Just ensure the device you choose has enough clock speed; otherwise it will cause your network to lag.

* **Host-Based Intrusion Detection System (HIDS)**

Instead of examining the traffic, host-based intrusion detection systems examine the events on a computer connected to your network, by looking into admin file data. This usually includes configuration and log files. A HIDS will back up your configuration files, so you can restore previous settings if a virus affects system security by altering the device setup. You'll also want to defend yourself against root access on Unix-like platforms or Windows system registry changes. A HIDS can't block these alterations, but it should notify you so you can act to rectify or prevent them.

Hosts monitored by HIDSs must have software installed. Your HIDS can monitor just one device if you'd like, but it's common to install a HIDS on every piece of equipment connected to your network. This prevents any configuration changes on devices from being overlooked. However, if you have a HIDS on every device, logging in to each one individually to access data is time-consuming and labor-intensive. That's why you'll need a distributed HIDS system with a centralized console or control module, so you can view the feedback for each host from one location. It is important for the system you choose to encrypt the information passing between the hosts and the centralized console.

NIDS vs. HIDS

So, should you opt for a NIDS or a HIDS? The short answer: you should probably have both. A NIDS gives you far more monitoring capacity than a HIDS can, allowing you to intercept cyberattacks in real time. A HIDS, on the other hand, is only able to identify if something is wrong once a setting or file has already been altered. By combining these two systems, you can achieve a preventive and responsive solution. Having a HIDS is important because HIDS activity is less aggressive than NIDS activity—for a start, a HIDS should not use as much CPU. Neither type of system generates network traffic.

TYPES OF INTRUSION DETECTION METHODOLOGIES

Both a host-based intrusion detection system and a network-based intrusion detection system will have two modes of operation: signature-based and anomaly-based. Almost all IDSs use both modes, though some may only use one or the other.

* **Signature-Based IDS**

The signature-based approach to IDS focuses on identifying a "signature" of an intrusion event. This could be in the form of a known identity, or perhaps a pattern. Most IDSs use the signature-based approach.

For this mode to be successful, it needs to be updated regularly, so it understands which identities and signatures are common. These identities and signatures are changing and evolving. In other words, if an attacker changes details about how the attack is executed regularly enough, they may be able to evade the attention of a signature-based IDS, because the IDS cannot keep up with the alterations. Brand-new attack types may also slip through, because they don't yet exist in the IDS database. Bear in mind, as the database grows, the processing load gets higher.

* **Anomaly-Based IDS**

Anomaly-based detection, as its name suggests, focuses on identifying unexpected or unusual patterns of activities. This method compensates for any attacks that slip past the signature-based model's pattern identifying approach. However, previously unknown but nonetheless valid behavior can sometimes be flagged accidentally.

Anomaly-based IDS is good for identifying when someone is sweeping or probing a network, which can provide a strong indication of an imminent attack. Examples of an anomaly include multiple failed login attempts and unusual port activity.

With NIDSs, an anomaly-based approach means you will need to establish a behavior baseline, so the system knows what's considered "standard" activity. This assists the system in flagging anything that does not fit in, or that would be considered abnormal.

* **Signature-Based vs. Anomaly-Based IDS**

The signature-based methodology tends to be faster than anomaly-based detection, but ultimately a comprehensive intrusion detection software program needs to offer both signature and anomaly procedures. This is because there are merits and disadvantages to both signature-based and anomaly-based intrusion detection software, which are largely compensated for when the two are combined.

HOW TO USE AN IPS

IPS is short for "intrusion prevention system." IPS and IDS software are branches of the same tree, and they harness similar technologies. Detection facilitates prevention, so IPSs and IDSs must work in combination to be successful.

The key difference between these intrusion systems is one is active, and the other is passive. A typical intrusion monitor alerting you when something is unusual or suspicious might be referred to as a passive IDS. A system that detects and acts to prevent damage and further attacks would be referred to as reactive. This is because it reacts to the intrusion rather than merely identifying it.[27]

A reactive IPS or IDS does not typically implement solutions itself but communicates with applications and firewalls by tweaking their settings. A reactive HIDS can communicate with multiple network aids, with the aim of restoring device settings. This could be SNMP settings, or the settings of a configuration manager installed on the device. If an attack is launched on the administrator, this cannot be responded to with an automatic block on admin use, or by altering the password for the system. This is because doing so would lock the root user out of the servers and network.[27]

IDS users sometimes complain they get floods of false positives when they first set up the IDS. Your IPS will implement a defense strategy automatically, based on the detection of alert conditions and thresholds. If the IPS isn't calibrated correctly, this can cause chaos and result in your authentic network activity halting entirely.

You can reduce the number of false positives, and minimize disruption to the network, by implementing your IDS and IPS in stages. You can customize triggers, combine warning conditions, and create tailored alerts. By combining conditions, they become more complex, which can reduce the likelihood of false positives occurring.

It's difficult, however, to eradicate false positives entirely without risking suspicious activity slipping through your defenses. You should aim for striking a fair balance, without compromising your security. Intrusion detection and prevention processes should be able to interact with firewalls in a fine-tuned way, to ensure genuine users aren't locked out and authentic network activity is not disrupted.

Challenges of Managing an IDS

There are three main challenges associated with managing an IDS. When choosing your intrusion detection software, look for a program that minimizes these challenges as much as possible.

Identifying false positives. The first challenge concerns the identification of false positives, which I've already 2addressed in part. False positives can put pressure on IT teams, who must update their IDS continually, so it has the information required to detect genuine threats and distinguish those threats from genuine traffic. This is a constant battle against false positives, which is time-consuming and labor-intensive. If the IDS is not up to date and suitably fine-tuned, which takes a lot of time in and of itself, then more time is lost coping with false positives.[27]

Many organizations use a secondary analysis platform, like a security incident and event manager, to help them analyze and investigate alerts in a more efficient way. Essentially, when an IDS generates an alert, it's sent to the secondary analysis system, which helps contend with the issue of false positives.

Staffing. The second issue is staffing. Understanding the context of threats and suspicious activity is an extremely important aspect of IDS management. The wider context is changing every day, as cybercriminals try to keep pace with security software. In addition, every IDS is implemented within the specific context of the organization in question.

To manage the complexities of the business-specific context and the wider context, you must have access to a knowledgeable and trained system analyst. The IDS analyst will tailor the IDS to the context but finding someone who has the credentials and experience to do this effectively is no easy task.[27]

Identifying genuine risks. False positives can be time-consuming and cumbersome but missing a legitimate threat can be worse. With an IDS, you have to know the nature of the attack to identify and prevent it. Experts refer to this as the "patient zero" problem: someone has to get sick before you can identify the illness in the future.

These are the three key challenges intrusion detection software is always trying to combat. Some tools do this better than others. Read on to check out the intrusion detection software programs I've found to be the most effective at managing these challenges.[27]

Typical Misconception about Antivirus

Nearly every office job requires the use of a computer, and while most people know how to operate one, they become lost when it comes to viruses and antivirus software.

However, this may be because there are several myths, misconceptions, and downright lies about virus and antivirus software that have thrown people off for years.

We here at Up and Running Computer Solutions have compiled a list of the most common myths and misconceptions about virus and antivirus software:

Myth #1: Error messages mean you have a virus.

People typically assume their computer has a virus when error messages begin to pop-up on their computer screen. That's not always the case though, error messages can be caused by other computer problems such as a faulty hard drive, bugs in the software or even problems with your antivirus software. The same applies when your computer crashes, it's likely caused by something other than a virus.

If you are getting error messages don't go from A to Z, try checking for any updates and cleaning your hard drive up to see if it helps. You can also scan your computer just to be sure that your computer isn't infected with a virus.[28]

Myth #2: Computers can infect themselves with a virus.

As silly as that sounds, many believe this myth. It's not uncommon for clients to bring in their computers claiming that a virus magically appeared on their system all on its own. However, viruses don't magically appear on computers, users must physically open an infected program, or visit a website that hosts an actual virus and download it.[28]

The best way to decrease the chances of your computer becoming infected with a virus is to avoid websites that contain illegal or "adult' content. Although other websites can be just as capable of hosting a viruses as well, so be cautious when sketchy sites offer free downloads.

Myth #3: Every antivirus software is the same.

While many people know how to operate computers, they are often confused when it comes to the antivirus software. They want to protect their computer, but only download free antivirus software or keep the one that comes preinstalled on their new computer. Most of the free antivirus software only protect against known threats though.[28]

The free antivirus software doesn't always protect against scan social media walls, phishing attacks or offer any mobile protection, and if your computer does get a virus, it may be very difficult to remove. There are even paid program that vary in their protection capabilities, so be sure to do your research and install an antivirus that best suits how you use your computer.

Myth #4: All computer viruses are the same.

This completely untrue. There are some viruses or malware that allow hackers to steal information. Some spread advertisements or spam, while others are much more atrocious, destroying your entire operating system, leaving it useless.

There are new virus that released all of the time, and they are all different. The best thing you can do is to be aware, follow the best security practices, and use an effective antivirus software to protect yourself and your computer.

Myth #5: Firewalls protect against computer viruses.

Wrong again, a fire wall is not an antivirus software. Firewalls manage traffic traveling over a network, but they do not protect again viruses, malware or Trojans. A firewall is a part of a smart security plan, and you should have one, especially if you use public networks. However, as mentioned, it will not protect your machine from getting infected.

Whether you need a virus removed or worried about your network security, Up and Running Computers Solutions is the place to call. Give us a call at 951-737-8558 and our experienced team will be happy to help get your machine back up and running. Or visit www.urce.net for information regarding our services.

Up and Running Computer Solutions proudly serves Corona, Riverside, Anaheim, Irvine, Newport Beach, Tustin and all surrounding areas.[28]

EVOLUTION OF ANTIVIRUSES

Before concentrating on the exact observe approximately antivirus software program, let's throw a few mild at the evolution of antiviruses. First viruses and antivirus have been created in remoted environments [2]. In 1971 a well-known laptop scientist named Bob Thomas created an experimental software referred to as the Creeper on the BBN Technologies, USA [2]. The Creeper software moved throughout the Digital Equipment Corporation's PDP-10 mainframe computers, which have been strolling the TENEX running gadget, and used the ARPANET community, which turned into a predecessor of the Internet [2]. What the Creeper virus did turn into it inflamed a far-flung laptop through the message "I'M THE CREEPER: CATCH ME IF YOU CAN!" was copied by ARPNET. [3].

The identical year, every other laptop scientist named Ray Tomlinson, who turned into additionally the co-employee of Bob Thomas, wrote a new edition of the Creeper, which replicated itself because it moved throughout the community rather than simply moving [2]. To get rid of the Creeper from the community, Ray Tomlinson wrote every other software referred to as the Reaper [2]. The Reaper moved throughout the ARPANET community, detected, and eliminated the self-replicating Creeper software [2]. The Reaper software turned into now no longer just like the anti-virus packages we recognize today, however, in truth, turned into an epidemic itself in that it turned into self-replicating and unfolds via a community [3]. Creeper and Reaper are taken into consideration to be the primary virus and antivirus.

Later while evolution started out in 1987 and honestly matters commenced to extra de withinside the antivirus industry, the primary elimination of an "in-the-wild" laptop virus referred to as Vienna Virus turned into carried out through a German protection professional Bernd Fix in 1987[2].

WHY ANTIVIRUS IS NECESSARY

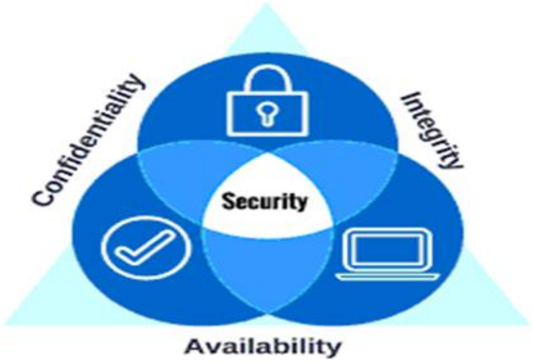
The predominant difficulty is the safety of 1's non-public records. If any unauthorized individual makes use of our records, then the scenario maybe worst. Basically, records protection is involved in 3 essential areas.

The CIA Triad of confidentiality, integrity, and availability are taken into consideration as the center underpinning of records protection [6]. Every protection management and each protection vulnerability may be considered in mild of 1 or extra of those key concepts [6].

- **Confidentiality:** It guarantees that non-public or exclusive records aren't always being shared with an unauthorized individual.

- **Integrity:** It guarantees that the information and gadget are blanketed from unauthorized manipulation.
- **Availability:** It guarantees that the gadget works nicely in order that it cannot deny legal users.

FIGURE Shows CIA Triad [5]



CONFIDENTIALITY

Confidentiality ensures that your personal and personal statistics are not constantly shared with any unauthorized individual. Most statistics systems house statistics that have some diplomas of sensitivity. It might be proprietary industrial organization statistics that the opposition may also need to apply to their gain, or personal statistics regarding an enterprise's employees, clients, or clients. Confidential statistics often have fees and systems are therefore underneath not unusual place attack as criminals hunt for vulnerabilities to exploit. Threat vectors include direct attacks which encompass stealing passwords and taking pictures of network visitors and additional layered attacks which encompass social engineering and phishing. A few styles of common area accidental breaches include emailing sensitive statistics to the wrong recipient, publishing personal information to public net servers, and leaving non-public statistics displayed on an unattended computer display screen [6].

INTEGRITY

Integrity measures shield statistics in opposition to unauthorized alteration. These measures provide a guarantee withinside the accuracy and completeness of the information. They need to shield statistics consisting of every truth that is stored on systems and information that is transmitted amongst systems that encompass email. In preserving the integrity, it isn't best crucial to manipulate get entry to at the machine level but to further ensure that machine clients are best able to adjust statistics that they'll be legitimately prison to adjust. As with confidentiality protection, the protection of information integrity extends beyond intentional breaches. Effective integrity countermeasures should moreover shield in the direction of accidental alteration, which incorporates non-public errors or information loss that can be given up the end result of a machine malfunction.[6]

AVAILABILITY

In order for a statistics machine to be beneficial, it ought available to prison clients. Availability measures shield well-timed and uninterrupted get entry to the machine. Some of the most crucial threats to availability are non-malicious in nature and include hardware failures, unscheduled software program software downtime, and network bandwidth issues. Malicious attacks include several varieties of sabotage supposed to reason harm to an enterprise through a manner of denying clients get entry to the statistics machine. The availability and responsiveness of a web website online are immoderate precedence for masses of industrial enterprises. Disruption of net websites to be had for even a short time can purpose a loss of revenue, purchaser dissatisfaction, and popularity harm. The Denial of Service (DoS) attack is a manner often used by hackers to disrupt net vendors. In a DoS attack, hackers flood a server with superfluous requests, overwhelming the server and degrading vendors for legitimate clients. Over the years, provider organizations have superior cutting-edge countermeasures for detecting and protecting in the direction of DoS attacks, but, hackers moreover keep gaining in sophistication and such attacks remain an ongoing difficulty. Availability countermeasures to shield machine availability are in an extended manner ranging due to the threats to availability. Systems that have an immoderate requirement for non-forestall uptime need to have vast hardware redundancy with backup servers and information storage proper now available. For large, enterprise systems it is a mile's common area to have redundant systems in separate physical locations. Software gadgets need to be withinside the vicinity to display screen machine average overall performance and network visitors. Countermeasures to shield in opposition to DoS attacks include firewalls and routers.[6]

ANTIVIRUS DETECTION SCHEME

For antiviruses, a signature is a set of rules or hash that uniquely identifies a selected virus. Depending on the sort of scanner being used, it could be a static hash which, in its best shape, is a calculated numerical cost of a snippet of code specific to the virus [7]. Javier [8] said that a plague signature has to be understood how a dependable manner to locate a number inflamed through concrete malware. It encapsulates the essence of a plague. Signature detection is complicated and tough however we can hold the focal point at the want of accumulating an easy signature collectively with associated context facts [9].

With the various antiviruses withinside the marketplace today, diverse mechanisms were hired through them to locate and control viruses as an instance with static analysis, a plague is detected through inspecting the documents or statistics for the occurrences of virus styles without simply going for walks any code. Static Methods consist of the subsequent methods [9].

The antivirus software program generally scans documents or your laptop's reminiscence for positive styles that could imply the presence of malicious software programs consisting of viruses. They consequently search for the presence of styles primarily based totally on the signatures or definitions of recognized malware. The virus sample to be had on a patron laptop relies upon the experiment technique the patron is the usage of. According to a booklet through IBM at the Trend Micro Pattern Files and Scan Engine (2015). The Virus Pattern incorporates facts that allow Core Protection Module to pick out today's virus/malware and blended risk attacks. For maximum antiviruses withinside the marketplace today, the maximum not unusual place shape of detection of viruses is a heuristic-primarily based totally detection that uses algorithms to examine the signature or styles of recognized viruses towards a capacity risk. The heuristic-primarily based totally detection lets the antiviruses locate viruses that have now no longer been determined or preceding viruses that have been changed or disguised and launched as a brand-new virus. This detection technique is the quality-recognized technique for detecting new viruses however at instances it additionally generates fake advantageous fits which means an antivirus scanner may also file a record as being inflamed that isn't always inflamed. Further, still, laptop desire booklet suggests that each antivirus scanner has a plague definition record, database, or dictionary that incorporates heaps of recognized virus signatures. These signatures permit an antivirus application to pick out beyond viruses that have been analyzed through safety professionals. For this, any other virus detection technique consists of the signature-primarily based totally detection approach. This is an amazing manner to save you beyond recognized viruses and is a quality technique of detection without developing a fake warning. However, signature-primarily based totally detection cannot locate new viruses till the definition record is up to date with new virus facts [9].

Other sorts of antiviruses rent conduct-primarily based totally detection mechanism to locate viruses. This is a completely unique string of bits, or the binary sample, of a plague. The virus signature functions similarly to a fingerprint in that it can be used to identify and locate specific infections.

The anti-virus software program makes use of the virus signature to experiment for the presence of malicious code. Behavior-primarily based totally intrusion detection strategies anticipates that an intrusion may be detected through looking at a deviation from ordinary or predicted conduct of the gadget or the users [9].

CONCLUSION

When we continue any paintings on laptop gadgets, we have to usually hold in thoughts that every time our gadget may be stricken by viruses. Day through Day wide variety of various sorts of viruses are determined, they're getting extra effective with growing time. In order to shield our laptop from exclusive viruses, we have to take the right precautions like antiviruses and plenty of different means, which may be very easy. But there isn't always a hundred percentage assure that our gadget will usually be virus less. Nevertheless, we will limit the virus's connection through the usage of the right antiviruses or safety mechanisms. There are diverse antivirus applications are to be had for laptop person that is exclusive on the premise of usage of reminiscence, set up time, size, interface, etc.

REFERENCES

[1] Antivirus software, From Simple English Wikipedia, the free encyclopedia

[2] Who Invented the Antivirus? A History of Antivirus Software. 2nd March 2022 by Manish Sahay

[3] UKEssays. (November 2018). History of Antivirus Software.

[4] H. A. Khan, A. Syed, A. Mohammad and M. N. Halgamuge, "Computer virus and protection methods using lab analysis," 2017 IEEE 2nd International Conference on Big Data Analysis (ICBDA*)*, 2017, pp. 882-886, doi: 10.1109/ICBDA.2017.8078765

[5] https://securitymatters.utoronto.ca/resources/it-professionals/

[6] Confidentiality, Integrity And Availability – The CIA Triad

[7] Landesman, M. (2016, October 20). What is a Virus Signature? Retrieved from Lifewire Tech: https://www.lifewire.com/what-is-a-virus-signature-153629

[8] Mellid, J. M. (2014, April 19th). Detecting and removing computer virus with OCaml. Retrieved from http://javiermunhoz.com/blog/2014/04/19/detecting-and-removing-computer-virus-with-ocaml.html

[9] https://www.researchgate.net/publication/322552067Review_of_Viruses_and_Antivirus_Patterns

[10] 4 'Exotic' Programming Languages Popular With Malware Developers by Dice Staff .August 5, 2021

[11] Patil, Dr. Bhaskar & Joshi, Milind. (2012). A study of Past, Present Computer Virus & Perfor- mance of Selected Security Tools. Southern Economist. https://www.researchgate.net/publication/288725457_A_study_of_Past_Present_Computer_Virus_Perfor-_mance_of_Selected_Security_Tools

[12] A short history of computer viruses by Alex Uhde July 5, 2017 https://www.sentrian.com.au/blog/a-short-history-of-computer-viruses

[13] What is denial of service attack (DoS) ? https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

[14] Denial of Service attack and its type-GRAYCAMPUS

https://www.greycampus.com/opencampus/ethical-hacking/denial-of-service-attacks-and-its-types

[15] Introduction : Denial of Service attack (2022 Amazon Web services, Inc) https://docs.aws.amazon.com/whitepapers/latest/aws-best-practices-ddos-resiliency/introduction-denial-of-service-attacks.html

[16] Understanding Server Traffic Logs and detecting denial of service attck by SQL-Server-Team ,Published Mar 23 2019 04:39 PM https://techcommunity.microsoft.com/t5/sql-server-blog/understanding-server-traffic-logs-and-detecting-denial-of/ba-p/385529

[17] Yusirwan, Syarif. "Implementation of Malware Analysis using Static and Dynamic Analysis Method." (2015) https://www.semanticscholar.org/paper/Implementation-of-Malware-Analysis-using-Static-and-Yusirwan/ae14f0d365a74977efc23c8eb40270db8e880c1c

[18] 5 must have features of antivirus software by Bob Martin | Jul 21, 2016 | Antivirus, Data Security https://greatlakescomputer.com/blog/5-must-have-features-of-antivirus-software

[19] 5 key features of antivirus solutions for SMBs By Mirren McDade, January 26th, 2022 https://expertinsights.com/insights/top-5-key-features-of-antivirus-solutions-for-smbs/

[20] Antivirus fundamental: Viruses, signatures, disinfection byAlexey Malanov https://www.kaspersky.com/blog/signature-virus-disinfection/13233/#:~:text=A%20virus%20signature%20is%20a,sufficient%20to%20detect%20malicious%20files.

[21] What is a Signature? By 1997-2022 Sophos Ltd https://home.sophos.com/en-us/security-news/2020/what-is-a-signature

[22] 7 Best Intrusion Detection Software and Latest IDS Systems By Staff Contributor on February 18,2020 https://www.dnsstuff.com/network-intrusion-detection-software

[23] Common Myths About Computer Viruses and Antivirus Softwar Posted on April 25, 2016 by admin http://www.urcs.net/computer-solutions-computer-repair-ca/5-common-myths-about-computer-viruses-and-antivirus-software/