Abstract - The aim of this paper is to explore the hypothesis of a computer virus threat, and how destructive it can be if executed on a targeted machine. What are the possible counter measures to protect computers from these threats? In this study, we performed an analysis from the data extracted from different test of scenarios and labs conducted in a test environment. Information security risks associated with computer viruses can infect computers and other storage devices by copying themselves into a file and other executable programs. These file get infection and allow attackers to connect to target systems by using backdoors. The results of this study show that, the proper security implementations and the use of up to date operating systems patches and anti-virus programs helps users to prevent the loss of data and any viral attack on the system. Nevertheless, this observation could be used for further research in the network security and related fields; this study will also help computer users to use the possible steps and techniques to protect their systems and information from any possible attacks on their network systems.

Keywords-computer virus, computer threats, lab analysis

I. INTRODUCTION

Cyber security is the biggest concern in today’s world. This threat is increasing each day as information security researchers reveal new threats and security vulnerabilities in the technologies that are widely used, which puts the security at a higher risk [1]. The number of network attacks is at its highest level in last few years, the biggest threat to any computer system is computer virus which proves itself to be the most devastating and the most commonly found technique to compromise systems. Moreover, investigating a various security features [2-4] could be an interesting path to explore in the future to protect Big Data [5]. This research paper will address these threats and we will try to find out its operations and types of attacker who can use these tools to compromise the security system. Finally, we will discuss the tips and techniques that can prevent us from being infected by these malicious and sophisticated computer viruses.

A. Virus

Computer viruses are basically a computer code which is capable of copying itself to other files and performs the required tasks mentioned in it codes. Virus is the most commonly used terminology in discussions due to its nature. The most appropriate term we can use is self-replicating programs because in the beginning the intentions were to create an artificial intelligent program nonetheless later it was changed for different purposes. There are number of viruses which have their own purpose and propagation techniques [1]. The basic routines that are normally used in computer viruses, are as follows.

Functional diagram of a computer virus, which has search, copy and anti-detection routines to avoid any detection from anti-virus software is shown in Fig. 1. Fig. 2 representing the number of updates that Avast anti-virus software provides to its users which is increasing every month. Fig. 2 gives a better understanding of the databases getting new and more data about computer viruses every month which should be shared with every user to prevent them from any newer threats.

B. Global Statistics of Computer Viruses and Its Attacks

Here are some statistical data that will show some important information regarding computer viruses and its severity,

![Figure 1. Functional diagram of a computer virus, which has search, copy and anti-detection routines to avoid any detection from anti-virus software](image1.png)

![Figure 2. The increments in users' updates for virus definitions and signatures in last 12 months](image2.png)
Fig. 3 represents the number of domains infected every month. It is easily noticed that thousands of domains are being detected as this shows that they are infected by different kind of virus programs.

The global map (Fig. 5) is represents the countries whose internet users are highly under attack by computer viruses.

The above graph represents the number of attacks prevented by anti-virus software every month. The values vary each month nonetheless compares the last 2 months, April as there are more attacks than in march which indicates that the attacks are increasing again. These results show that the virus attacks and the infection of the systems are increasing rapidly and the number of threats is at its highest. These threats definitely need serious attention because these infected computer systems can further be used in other attacks. Infected computers are used as zombies, and attackers have complete control over it. Further we need to show you which computer systems and operating systems are under more threat and are likely to be infected compared to others.

Fig. 7 shows that the overall percentages in different categories of operating systems have a higher chance to get infected by the viruses than other operating systems. These results also show us that the most usable operating systems around the globe are operating systems that are inadvertently most infected.

These statistics show that the overall understanding of the threat and its nature and the fact that no communicating device is completely protected. We need to develop a software programs that needs to be sophisticated enough to detect these viruses and block them from spreading. Although there are number of Anti-Virus software tools that run on different machines and protect
them from different viruses the hidden Trojan software uses different methods and it is still not enough to say that they are fully protected.

C. Anti-Virus Programs

There are number of anti-virus programs that detect, block and delete any malicious programs that are running in the systems. There are four mechanism and techniques that are being used by anti-virus softwares which are: (i) Signature based detection (ii) Heuristic-based detection (iii) Behavioral based detection and (iv) Cloud-based detection.

1) **Signature based detection:** Signature based detection is an essential technique of the anti-virus programs. This method operates on matching of fingerprints to the file with the signature of the virus; signature is a series of bytes in the file. Although this technique has drawbacks like it cannot flag the malicious file if the signature of the new virus is not created yet, it is still more promising than other ones in the market.

2) **Heuristic-based detection:** In this technique anti-virus programs operate by examining the static file for any suspicious characteristics without an exact signature match. This technique may also flag a legitimate file as malicious.

3) **Behavioural-based detection:** Behavioural-based detection works by observing suspicious behaviours of the file. This method operates by executing and unpacking the malcode and it listens to the keystrokes etc., this technique give anti-virus program the ability to detect any malicious program in the computer system [6].

4) **Cloud-based detection:** Cloud-based techniques identify malware by collecting data from different protected computers and analyzes all the data on the provider’s systems and sends results to the clients’ system. The decision is made on the clients’ local system by analyzing the characteristics and behavioristics of the client [6].

II. MATERIALS & METHOD

For this research a pragmatic approach was used to get the required results, and techniques like qualitative method is used to extract information about the computer viruses and their source codes to analyze and know, how a basic computer virus works and the basic components of virus operate [7]. This will lead the research from the very basic mechanism of the computer virus to the one of the advanced and sophisticated virus codes which can trick an anti-virus and disable its functionalities [8]. This also shows what tools a hacker can use to extract interesting data from the victim’s machine. After getting the required information it was applied to those codes to compile it as a working computer virus. A test computer virus was created to study the working of a virus where it demonstrates destructive and non-destructive behaviours. This paper has also studied the possible defend mechanisms and techniques to prevent such infection to our computer systems.

Test environment

In our test environment we used virtual machines to perform our testing, we used different software’s to create viruses that gave us options to select the type of virus and payloads we want to use, in our scenario, and we used the following software tools,

**Virus construction tools** (i) Virus maker, (ii) JPS virus making tool, (iii) Internet worm maker thing

In this testing, we created a virus by choosing the specific payloads and functions and saved it on the test computer, which was ready to invade computers by just sending them to the target machine. The purpose of these tests is to observe the operations of different anti-virus programs to assess if they are able to detect and block such threat and if yes, then what will be the ratio of this success.

**Virus payload Trigger mechanism:**

Virus can use different trigger mechanisms to launch their attacks on the system or perform any task, if there are a number of triggering mechanisms, such as, (i) The counter trigger (ii) Keystroke counter, (iii) Time trigger, and (iv) The system parameter trigger. There are number of other logics that are used in the viruses to perform any required task, few of the logical payloads are


To analyze the virus, we used IDA and ollyDbg software which provide the result in order to study the ability and structure of a computer virus.

**Creation of computer virus**

To create a virus to test these environment JPS virus maker 3.0 was used, which provides the number options to select the payloads. In this scenario the most basic payload was selected like to mute the computer sound. Other payloads were also tested on the system.

**Analysing Virus**

Analyzing computer virus is always a bigger task and it requires some expertise [9]. Here IDA and ollyDbg were used for analyzing our virus.

[Figure 8. JPS Virus Maker GUI for designing our test virus.](image-url)
After selecting all the options and doing the requirements we finally created our virus.

<table>
<thead>
<tr>
<th>Software</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>JPS Virus Maker 3.0</td>
<td>Used for creating test virus</td>
</tr>
<tr>
<td>IDA</td>
<td>Used to get the flow chart and routines of the test virus</td>
</tr>
<tr>
<td>OllyDbg</td>
<td>Used to extract the source code of the test virus</td>
</tr>
</tbody>
</table>

### III. RESULTS

The findings were surprisingly shocking as it was found that there is no such computer anti-virus software that can prevent targeting the system from every virus attack [10]. There are number of limitations of anti-virus programs either due to its procedures and defending mechanism or due to the lack of information about the certain virus codes which remain undetectable some period of time. Any new attacks will definitely take some time to recognize and to design the defending mechanism for the protection of such attack. Furthermore, all the anti-virus programs use their databases for getting updates; any new attacks will take some time for security experts to update. The database and to apply those security measures, the time period in which there is no security measures, the virus programs will be free and can perform much advance destructions.

### Creation of worm

Worm is the type of computer virus that can infect every file in the system and is the most devastating type of threat because of its nature and it can escape from one machine to another and can also infect other computers [11]. The basic mechanism of the computer worm is to replicate itself with timely proportion and will affect the CPU in such a way that it will no longer be usable and it will finally crush. The equation for the worm infection is, $y = x^t$ where, $y$ is total number of worms in the computer system, $x$ is the number of worms in current time, and $t$ is the time period in seconds.

![Figure 10](image1.png)

Figure 10. The number of worms in an infected system after 30 secs of being infected.

Fig. 10 represents the propagation of worms in targeted system after 30 seconds of infection. This will grow exponentially and will use all the system resources.

There are thousands of computer viruses in the internet that are infecting files and other computer programs and softwares which results in the spreading of these viruses [10]. No computer system is considered safe and it gets infected as long as it is connected to the internet. Accessing websites and downloading files from the internet is the biggest cause of computer infections. There are number of viruses which are hiding inside the legitimate looking programs and waiting for you to download them as they will perform their task in a pre-programmed way [7]. For designing any computer virus, it is essential to know which type of files are going to infect and how it will perform its search and copy mechanism, and how different viruses infects different file formats to perform the tasks according to their payload [9]. It is essential to adopt a multi-layer security approach for protecting networks and computer systems.

In a multi-layered security which recommends to use a specialize devices and the software with proper updates, Fig. 11 represents five layers of security approaches which includes, (i) Network Firewall and IPS, (ii) OS firewall (iii) Anti-Virus Software (iv) Behavioral Detection, and (v) OS security patches.

### Monitoring System

Malware and Trojans tools create a backdoor in the system and that allows hackers to remotely control and use your computer system. It is always essential to monitor your system resource utilizations and your network connections. If it finds any unwanted or unknown connections in the server or other computer machine over the internet, then it always recommends disconnecting the session immediately. It also blocks unwanted and unnecessary ports as well, as this will minimize the attack scope for any hacker. There are number of tools that are available for this purpose and most easily available tools is `netstat` which will provide you with all the required information regarding TCP/IP connections.

### IV. CONCLUSION

In this paper we performed an analysis of the data obtained from the different sources and scientific literature, and discussed the potential effects of a computer virus on the computer system that can be serious if it is not addressed
properly. Different tests were performed in a lab environment where the operations of the computer viruses were analyzed and their different techniques were used to propagate it into the systems. This study provides the possible solutions which will help other people to protect their systems from any damage. This data implies that the hypotheses of computer systems can easily get infected by computer viruses. However, due to the limited resources available for the test environment it may be safer to look at other possible explanation. One limitation to this study is that we could not test all the possible computer viruses and other malicious codes to extract all possible results. **Source Code**

OllyDbg is used for extracting source code of the virus and to analyse its operations and routine.

---

**REFERENCES**


