**TABLE OF CONTENTS**

[WORLDS DEADLIEST COMPUTER VIRUSES AND WHY WE SHOULD BE AFRAID OF THE FUTURE OF THEM? 2](#_Toc66042214)

[ HISTORY 2](#_Toc66042215)

[ DEFINITION AND ITS IDENTIFICATION 2](#_Toc66042216)

[ HOW DIFFERENT TYPES OF VIRUSES AFFECT COMPUTERS? 2](#_Toc66042217)

[ MOST DEADLY COMPUTER VIRUSES AND THEIR FEATURES 3](#_Toc66042218)

[CRYPTOLOCKER 3](#_Toc66042219)

[PLUGX 4](#_Toc66042220)

[Zeus Gameover 4](#_Toc66042221)

[Nimba 4](#_Toc66042222)

[ILOVEYOU 4](#_Toc66042223)

[ WHAT IS THE FUTURE OF VIRUSES? 4](#_Toc66042224)

[ CAN THIS FUTURE BE PREVENTED? 5](#_Toc66042225)

# WORLDS DEADLIEST COMPUTER VIRUSES AND WHY WE SHOULD BE AFRAID OF THE FUTURE OF THEM?

## HISTORY

Computer viruses have been around as for quite a long time and it is proved by the fact that the first computer virus was detected in the 1970s ARPANET which was the first developed phase of the internet. The name of this virus was “Creeper” which was created by Bob Thomas in 1971. In early times, TENEX operating system was used by computers and TENEX was the main target of Creeper. Creeper used to enter computers through ARPANET and then it used to copy itself infinite times showing a message "I'm the creeper, catch me if you can!". However, it was not long when finally a cure for this virus was created which was known as THE REAPER and it effectively deleted Creeper from the systems.

However, with the passage of time, operating systems of computers kept developing and then IBM came into being. We know that as technology is developing day by day rapidly so are the ways to infect new technology. Amjad Farooq Alvi and Basit Farooq Alvi who used to live in Lahore, Pakistan used to run a computer store. When they detected that the software written by them is getting copied by others, they made the first IBM PC virus which was named “Brain”. The brain was created in 1986 and its purpose was to show a mystery copyright message instead of damaging any data. Moreover, after discussing the ancient PCs, it’s time to tell about the first virus to target Microsoft windows. The first virus to target windows was discovered in 1992, and it was named as WinVir. It did not have any serious danger towards windows instead it was just replying on messing up the DOS.

## DEFINITION AND ITS IDENTIFICATION

As human beings get infected by viruses in the form of flu or cough which disturbs their proper body functioning then they have to take medicine to get treated by it. A computer virus is similar to that. It enters the computer operating system and infects its several files and folders which disturbs the computer's usual processing and users have to perform certain actions to free their computer from viruses. In more professional terms, “A computer virus is a malicious software program loaded onto a user’s computer without the user’s knowledge and performs malicious actions.” It is basically designed to damage others’ devices or even steals data as well.

When a computer gets infected by a virus there are several ways to recognize that your computer is infected by a virus which includes slowing down of the computer, not working up to its mark. Or unexpected data loss and frequent computer crashes are also one of the signs showing that your computer is infected by malware or a virus now. Another sign of proving that your computer is infected is that there will be a random installation of programs in your computer or your computer password might get changed randomly as well.

## HOW DIFFERENT TYPES OF VIRUSES AFFECT COMPUTERS?

Computer viruses are of different types and they can affect your computer in different ways as well. I will be discussing a few of them which includes:

1. Resident viruses

This type of virus disturbs the system operations of your computer and targets the RAM. This virus is very clever in that it can even make itself look like an anti-virus program as well and will get attached to anti-virus software files and will get undetected by viruses’ scans.

1. Multipartite virus

Unlike a resident virus, this virus affects the entire system. It can affect the operating system, the privacy, folders, or even programs as well of your computer.

1. Direct action virus

This kind of virus only attaches itself to a specific file of .exe extension which means that it is easier to detect and remove without any serious damage.

1. Browser hijacker

These viruses' purpose is to annoy you while you are using your web browser and how it affects you is by redirecting you to malicious websites.

1. Overwrite virus

As the name suggests, this virus will overwrite files to infect folders, files or programs as well. It is a common type of virus that can be easily found in computers. It can get transferred through DVDs or USBs as well easily.

1. Web scripting virus

This virus is a clever one as it hides itself in the coding of links, ads, images or videos as well. And after it enters your computer, it will start infecting your files and this virus is hard to discover or identify.

## MOST DEADLY COMPUTER VIRUSES AND THEIR FEATURES

After discussing everything basic about viruses, it is time to discuss the most deadly computer viruses and what dangerous features they are having. There are several which are as following:

### CRYPTO LOCKER

This is a different and unique type of virus. It was developed in 2013. What it does is that it enters your computer through email attachments and puts a lock or password on your files and then you would have to pay an amount in order to recover your files or documents. After paying the required amount, you will be provided with a specific key to unlock your file. If you do not pay for your file then the data placed in your folder is lost forever. An example of this virus demonstration is that in 2014, Evgeniy Bogachev, leader of CryptoLocker was taken down and the FBI offered a price of $3 million as a price for capturing Bogachev.

### PLUGX

This virus is specifically built for government bodies. PlugX is a Remote Access Trojan (RAT) which is also known as “Korplug”. This virus's main target is government entities, targets specific businesses and organizations. The attack starts with a phishing email containing a malicious attachment, usually, a specially crafted malicious document, and exploits a vulnerability in either Adobe Acrobat Reader or Microsoft Word.

### Zeus Gameover

This virus belongs to the “Zeus” family of viruses, discovered in 2011. It basically deals with money. This virus will enter your computer through either spam messages or drive-by downloads. This virus tries to locate bank account details stored in your computer and will hack them. The virus creates a server to send the hacked information back to its developer.

### Nimba

This was a very dangerous virus during its initial days however it still is a dangerous virus. It was first detected in 2001 and it moves around through the internet. During its initial identification, it took Nimba 22 minutes to become the worlds’ most deadly virus. It basically brings internet traffic to a crawl. It creates a hidden passage in other persons’ computers and gives access to its developer. Now the developer can do anything with your computer including checking all the information or even taking full control of your device as well.

ILOVEYOU

As the name suggests, it appears to be a cute virus with not many deadly effects however, this virus is among the list of deadly viruses for a virus. ILOVEYOU virus originated in the Philippines, began to infect computers on May 5, 2000. The virus spreads by email with the subject line “ILOVEYOU” and an attachment, “LOVE-LETTER-FOR-YOU.txt.vbs” If the attachment was opened, a Visual Basic script was executed, and the computer was infected. It was managed to wreak havoc on computer systems all over the world with around $10 billion worth of damages. 10% of the world’s computers were believed to have been infected. It was so bad that governments and large corporations took their mailing system offline to prevent infection.

## WHAT IS THE FUTURE OF VIRUSES?

Computer viruses have been around us for a long period of time however, in the ancient history of viruses, they were not that dangerous or were easily detectable and removable, however, with the advancement in technology, computer viruses are something which might be the reason behind the destruction of our earth as well. Today, computer viruses are having more consequences, and the objective of their developers is also changed and much frightening now. Before viruses were used only to piss someone off or to deliver a non-stop message which will always keep popping up on your screen. But now viruses are used to demand money, to hack government official computers, hack nuclear codes and threaten a country on basis of leaking those codes. The fact that the future of viruses will be frightening can be proved by saying that upcoming viruses will be invisible or simply undetected. And in order to prevent a device from getting hacked, you would have to think of every method by which your device might get infected and this is very much difficult to do. However, if you simply want to hack a device, then you have to just find a single way that the user has not yet thought of and you can simply hack his device now. Another thing that should be brought under consideration is that will future viruses be able to infect humans as well? Without the advancement in technology such as nanobots or AI, imagine someone infecting your robot with a virus and they end up killing you without even realizing what they are doing. This possible reason might end up in bio-wars with hacked nanobots or viruses on both sides.

Considering the fact that computer viruses might be the future of war then one thing is understood that viruses are no longer an innocent program. Who knows hackers might end up hacking your military headquarters and forward that sensitive information to your enemies at a higher price. Which eventually, will benefit the hacker and the enemy state as well.

There is even a case with Estonia as well. Estonia is the first nation to succumb to a huge-level web assault. In April 2007, the Estonian Government chose to eliminate a Soviet war commemoration from the focal point of the capital despite various protests. As an outcome, there were assaults on different government sites through programmed, repeating demands, something which is known as Distributed Denial Of Service (DDOS). For around three weeks, the sites of the Estonian president, parliament, and services, just like those of significant banks and three of the six primary news organizations, were closed down because of over-burden.

## CAN THIS FUTURE BE PREVENTED?

No one knows what the future is but what we have expected can be prevented by taking some serious measures. The first one is to update the IT security system of every program which is almost impossible and a very intensive task to do. Yet again, there are not many ways to prevent cyber wars or getting your computer being infected by viruses because as mentioned earlier as well, if you want to protect your computer then you would have to cover every angle from which your computer might get infected however, for the virus developer, he just has to identify one loophole and boom your computer is infected by the virus once again. One possible way to save yourself from getting infected is by disconnecting your official computers from internet access. That will save your computer from a lot of possible threats because most of the viruses infect your pc through the internet or emails so this is how you can possibly save yourself.

### REFERENCES

1. <https://en.wikipedia.org/wiki/Computer_virus>
2. <https://www.webroot.com/us/en/resources/tips-articles/computer-security-threats-computer-viruses>
3. <https://us.norton.com/internetsecurity-malware-what-is-a-computer-virus.html>
4. <https://hightouchtechnologies.com/9-common-types-of-computer-viruses/>
5. <https://lifars.com/2020/04/top-10-most-dangerous-cyber-virus/>
6. <https://www.alumniportal-deutschland.org/en/science-research/news-from-science/cyberwar-computer-virus/>