

Virus

with C

Authors:

Charles Chayon Mondol (180208)

Abu Dawod Rahman (180216)

Rabiul Hasan Nayan (180234)

Muntaseer Hafiz (180239)

# What is a Computer Virus?

A computer virus is a malicious program that self-replicates by copying itself to another program. In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them.

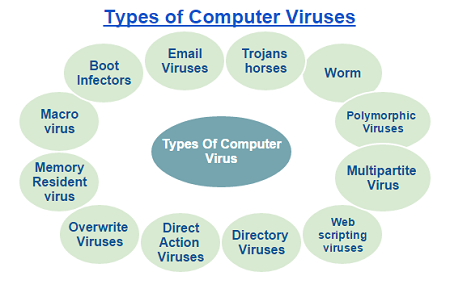
One of the ideal methods by which viruses spread is through emails – opening the attachment in the email, visiting an infected website, clicking on an executable file, or viewing an infected advertisement can cause the virus to spread to your system. Besides that, infections also spread while connecting with already infected removable storage devices, such as USB drives.

It is quite easy and simple for the viruses to sneak into a computer by dodging the defense systems. A successful breach can cause serious issues for the user such as infecting other resources or system software, modifying or deleting key functions or applications and copy/delete or encrypt data.

There are two types of ways in viruses operate, as soon as they land on a new device they begin replicating, while the second type plays dead until a particular trigger makes the malicious code to be executed. Thereby, it is highly important to stay protected by installing a robust antivirus program.

Presently, the sophisticated ones come with evasion capabilities that help in bypassing antivirus software and other advanced levels of defenses. Subsequently, the polymorphic malware development in the recent times enables the viruses to dynamically change its code as it spreads. This has made the virus detection and identification very challenging.

# Different Types of Virus:

* Boot Sector Virus.
* Web Scripting Virus.
* Browser Hijacker.
* Resident Virus.
* Direct Action Virus.
* Polymorphic Virus.
* File Infector Virus.
* Multipartite Virus.
* Macro Virus.

Among these types of viruses, we have tried to make some Direct-Action Viruses using only C language.

Here we have made 4 sample Direct-Action Viruses that uses

File directory access to manipulate, delete, copy and as well as making its own replica.

And almost all of them implements the header file dirent.h which enables us accessing through the file directories.

dirent.h

The <**dirent**.**h**> header defines the following data type through typedef: DIR. A type representing a directory stream. It also defines the structure **dirent** which includes the following members: ino\_t d\_ino file serial number char d\_name [] name of entry. The type ino\_t is defined as described in <sys/types.**h**>.

This header file is used in our codes and its library functions like readdir has been used for various purposes

We have created Four Viruses

* Self-Replicating Virus
* Copy Virus
* Memory eater
* Deleting Virus

All of them are Direct action Virus and they are controllable under certain circumstances.

We have also tested them on Windows operated machines and also in Virtual Box to avoid certain complexity and damage of the machines.

Self-Replicating Virus

This virus’s work is to replicate its own executive file in every folder of a partition. For making this virus we will need to work with directory. We need DIR type pointer to access directory and struct dirent type pointer. We will also need to work with strings and dynamically allocate memory. So, we will need stdio.h, stdlib.h, string.h, dirent.h header file.

LINK OF THE CODE IS GIVEN BELOW

<https://drive.google.com/open?id=1UaJfmt8XzZpSTEQCEAnObfFZqzKjmTNx&fbclid=IwAR2VT6bTX3_ycBt77Af-rj6VDwAkD9RARx3Erate6Hjf59PA2EQLuEZKhWE>

Here we only need to give this virus a path and it will make a copy of its own executive file in each folder including the path folder. Firstly, we need include stdio.h, stdlib.h, string.h, dirent.h header files.

In the main function we have just used a user defined function “replicate\_d”. Its return type is “void” and its parameter have a character type pointer. The formal view of this function is: “void replicate\_d (char \*str1)” We have also used three more user defined function named addstring, copy, fileorfolder. Formal view of these functions is:

char \*addstring (char \*str1, char \*str2)

It takes two-character type pointer as parameter and returns a character type pointer.

• Its work is to add two strings. The first pointer \*str1 points the first string. The second pointer \*str2 points the second string. This function just adds these two strings returns the joined string.

• In this function firstly, we have declared two integer len1 and len2 and assigned the length of the first string and the second string respectively. For doing this we have used “strlen” function.

• We have declared a character type pointer \*str and 3 integer type variable I, j, k;

• Then we have dynamically allocated memory to \*str. For this reason, we need “malloc” function. Malloc function dynamically allocates memory. Here we have allocated (len1+len2+1) numbered character type memory.

• Then we assigned two strings one after another by using loop and added a null character at the next memory of the last character. And have return the str.

int fileorfolder (char \*str)

It takes a character type pointer as parameter and returns an integer.

int copy (char \*str)

It takes a character type pointer as parameter and returns an integer. The work of four user defined functions are:

void replicate\_d (char \*str1)

We have worked with the directory in this function. We have opened the directory with opendir () function and read the file or folder of that directory with readdir () function. If an element is folder then we copy the main executive file in that folder. We have copied the main executive file with copy () function and figured out that element is file or folder with fileorfolder () function. We have used recursion to go through all the folders

int fileorfolder (char \*str)

Its work is to let us know if the given string is file or folder. • Firstly, we have assigned the length of the string which the parameter pointer indicates in an integer variable.

• If the string “.” or “..” the function will return 1 which means we don’t want to copy anything here. So, we have used control statement.

• Then we have checked the whole string using loop. If we can find ‘.’ character there then the function will return 1. Because it would be a file. It will be a folder if the string doesn’t contain any ‘.’. So, we have controlled this situation in a loop with control statement. If the loop executed completely then it will return 0. That means the string is a folder as it doesn’t have any ‘.’ character in it.

int copy (char \*str)

• In this function we have declared two FILE type pointers \*fp1 and \*fp2. We have opened the main executive file with “fopen ()” function and assigned it in fp1. Then we have used the addstring function and added two strings one of which is saved in “str” and another one is “Virus.exe” and assigned the function’s return value into str1. Here “str” is a path. For using “Virus.exe”, this virus copies the same .exe file as the main .exe file of the virus.

• Then we have opened and created a new file named “Virus.exe” and copied the full fp1 file to fp2.

• Then we have closed fp2. And used rewind () function so that we can copy the fp1 again.

Thus, this is how the Self-Replicating Virus operates.

………………………………………………………………………………………………….

Copy Virus

This Virus’s work is to make a folder in partitions so that the space in drives goes out. We have used stdio.h, string.h, stdlib.h header file.

LINK OF THE CODE IS GIVEN BELOW

<https://drive.google.com/open?id=1gE4odRZHaS6AqWSZWysPWjVYoiJNR95B&fbclid=IwAR2vfYauaDQ16uVE35jZeSdejxiaVZb5tMnrvoOyjACKAOTOUY2HbsAfFy4>

We have used take () user defined function to copy files into C drive, take\_d () user defined function to copy files into D drive and take\_e () user defined function to copy files into E drive. First, we have copied files into C drive. We can’t just copy file into C drive because windows do not give us permission. So, we have created a folder first there using mkdir () function, then we have copied files there. For D and E drive, we can copy files there so we have not created any folder there. In main function we have taken an array of characters to determine the file name because we cannot make files having same name. The user defined function’s work is to copy a specific file. We have passed the name to the file through the parameter. In the function we have gone through loop where files would be created. Here we have used fopen (), fclose (), rewind () functions to do that.

………………………………………………………………………………………………….

Memory Eater

This virus tests the capacity of operating system of creating folder. We can create folder in our machine because windows provide us that accessibility to do so.

But there a question arises how much?

So, this virus was made to test the fact actually how much indeed how long the windows can offer us to create folders.

So, this simple code starts creating directories by mkdir (char [] s) when it runs the console prints and the directories are made. After sometime like 2-3 sec the device feels a bit laggy and the after that it hangs and disrupts doing the simple commands like closing the program. Though the windows recover when we close it after crashing due to stack overflow

LINK OF THE CODE IS GIVEN BELOW

<https://drive.google.com/open?id=1EQCRVZXl-wlSAwWlXblaYUWzThAl5TEF&fbclid=IwAR31ZNxfP8m_7BUkELDEFevvM4ILJlJoiPlIbBwOJunQgLwrRt4mfDYfbzs>

here we have a screenshot while running the virus and a window of Task Manager that indicates that the virus consuming the disk space and making CPU deal a heavy load thus, causing lag and hang eventually.

This virus enables us to make infinite directory creating approach which most of the windows versions handle pretty well but faces certain lag during this and lower OS will crash due to stack overflow.

<https://drive.google.com/open?id=1wOfNfHgjXM6YiFS1vcZ1OSGg9WgS-BP_&fbclid=IwAR0oqlNwq8IRpZLbDhuox8i2o9013_iQztFGoBb-pwLos8MNP8hytJvQ2Cg>

………………………………………………………………………………………………….

Deleting Virus

This virus’s work is to delete the files of the folder including itself where it is stored of a partition. For making this virus we will need to work with directory. We need DIR type pointer to access directory and struct dirent type pointer. We will also need to work with elimination and check availability of file in those directories and being able to open as well as reading those directories. So, we will need stdio.h, stdlib.h, string.h, dirent.h header file.

LINK OF THE CODE IS GIVEN BELOW

<https://drive.google.com/open?id=1bvtm6QwPmi0B2PHARl-7J6O8p8-VPAVL&fbclid=IwAR19MBiSRMRTr7X3Y7vwFX4nt0sh_XZqtJjr5Q1IM5_jSR76NuAodmdSo5s>

Here we only need to give this virus a path and it will delete all the files and folders of that directory. Firstly, we need include stdio.h, stdlib.h, string.h, dirent.h header files.

Here we have made some user defined functions to make the process easy those are addstring (char \*s1, char \*s2) , fileOrDir(char\* aa) , deelet(char aa[])

char\* addString (char \*s1, char \*s2)

this function returns a string pointer that adds Strings s1 & s2 that are given in the parameter.

* We have dynamically allocated memory to \*str. For this reason, we need “malloc” function. Malloc function dynamically allocates memory. Here we have allocated (len1+len2+1) numbered character type memory.

• Then we assigned two strings one after another by using loop and added a null character at the next memory of the last character. And have return the str.

int fileOrDir (char\* aa)

this function checks the given string whether it’s a file or a directory. Usually it looks for ‘.’ In a string to determine the given string as a file or it will be a directory -

• It’s work is to let us know if the given string is file or folder. • Firstly, we have assigned the length of the string which the parameter pointer indicates in an integer variable.

• If the string “.” or “..” the function will return 1 which means we don’t want to copy anything here. So, we have used control statement.

• Then we have checked the whole string using loop. If we can find ‘.’ character there then the function will return 1. Because it would be a file. It will be a folder if the string doesn’t contain any ‘.’. So, we have controlled this situation in a loop with control statement. If the loop executed completely then it will return 0. That means the string is a folder as it doesn’t have any ‘.’ character in it.

int deelet (char aa [])

this function does the main part of this code by using the remove (char \*s) function to delete the files in other words making the files address to the memory undetectable and returns zero if successful. remove () is a function of stdio.h header file which enables us damaging the files of the selected path and the directory location where the virus is stored.

In this scope we try to open the directory the virus is stored in using opendir () & also apply a recursive way to read the directories through using readdir () if the directory is null then we move forward using addString (bb,” \\”) after that when we find a file while opening the directories we use the remove function that makes the files disappear and after that close the directory using closedir ()

In the main function we just have to copy the path of the virus where it consists and after running the program all the files of the directory will be deleted except the directories.

And surprisingly it happens fast and big amount of data can be deleted within 2-3 secs only. Moreover, the data that are damaged cannot be found in the recycle bin!

Through the execution the virus itself will be deleted by itself after every execution and only the .exe will be available.

We have also upgraded the virus to be able to remove the directories also and avoiding more time complexity the code runs very fast.

Caution

* The following viruses are tested and been proven to do what they are described this long.
* Please be cautious while trying and executing these programs it can cause uncoverable damage.
* It is advised to use Virtual Box to test these Viruses & avoid certain difficulties.