**How To Make Antivirus Using C++ ?**

There are many tutorials on the internet teaching you how to write virus programs that could destroy the basic configurations of any Operating System. But here at CodeMink, we’ll tell you how to make AntiVirus using C++. Although, you can write the code in any programming language of your choice, but we’ll focus the concept in C++.

**What’s the focus Point?**

The main point behind searching any virus is identifying the code structure of any virus file.

Suppose, we’ve found this following virus in computer,



Virus File: How to Make Antivirus in C++

Now we’ll see the Binary code of this file.

Simply open this file in your favorite text editor. I advise you to use Notepad++ for the purpose.

Upon opening the file, you’ll see all unknown characters in file. What you have to do is just concentrate on characters which are identifiable (consider the image below)



Virus exe File opened in Notepad++

**In the 1st line,**
**1st character** = M
**2nd character** = Z

**In 2nd line,**
**9th character** = P
**10th character** = E

**In 9th line,**
**3rd character** = (
**4th character** = %

Take at least 10-12 character samples from the file and write then in text file in the following format:



Virus Database

Now this file will act us our virus Database. We can simply update this file and supply to the user for a better protection.

**Let the Scanning Begin**

Now, suppose we’ve to scan **any user specified** folder. Let’s write code in C++ for the same.

For doing this, we need to:

* **STEP 1:** Get a list of all the files present in that folder including sub directories too.
* **STEP 2:** Scan them one by one using the character sample we’ve collected above. If the characters at positions specified above are matched with those in files, then it would be tagged as “Infected”.
* **STEP 3:** Delete the virus file, in case we find them.

**Its Coding Time Now:**

[cpp]/\*The program written below is an exclusive property of www.codemink.com
You are not allowed to copy/reprint it in any social media like:-
books, internet, blogs, etc. without the permission of its author.
Author: Lavneet Sharma
Release Date(dd/mm/yyy): 7/2/2013 \*/

#include <dirent.h>
#include <string.h>
#include <fstream.h>
#include <conio.h>
#include <stdio.h>
#include <stdlib.h>
#include <iostream.h>

int scan\_this(char \*file\_name)
{
char \*pattern, \*line\_in\_file;
char file\_ch, ch;
int val, val2, flag;
ifstream fin3, fin4;
fin3.open(file\_name); // incase the file is not accesible
if(!fin3) return 0;

else // file is accessible | 100% it is a file.
{
//Opening Virus Database File
fin4.open("db.txt"); // this is our character pattern file

for(;;)
{
fin4>>pattern;
if(!strcmp(pattern,"<-"))
{
fin4>>pattern;
if(!strcmpi(pattern,"End"))return -1;
else if(!strcmpi(pattern, "virus"))
{
if(flag) return 1;
else continue;
}
}
else if(!strcmpi(pattern,"LINE"))
{
fin4>>val; // got the line number

// skipping initial lines to reach the line number
for(int i=0;i<val-1;i++)
{
fin3.getline(line\_in\_file, 300);
}

fin4>>val; // got the character number
fin4>>file\_ch; // got the character

//skipping initial character to reach the character
for(i=0;i<val-1;i++)
{
fin3.get(ch);
}

if(file\_ch == ch) flag = 1; // matched.
else flag =0;
fin3.seekg(0); // set to start
}
}

}

}

void main()
{
char comm[300], dirpath[100], file\_name[200];
char ask;
int response;
ifstream fin;

cout<<"Enter Directory you want to scan: ";
cin>>dirpath;

strcpy(comm, "dir ");
strcat(comm, "dirpath /b /s >tmp.$$$");
system(comm);

fin.open("tmp.$$$");

while(!fin.eof())
{
fin.getline(file\_name, 200);
response = scan\_this(file\_name);
if(response == 1)
{
cout<<"<–!! Caution.! A Virus has been Detected..!";
cout<<"\n"<<file\_name;
cout<<"\nPress Enter Key to Delete it.";
ask= getch();
if(ask == 13)
{
remove(file\_name); // delete the virus
}
}
}

fin.close();
cout<<"Scan Complete.!! Thank You for using our anti virus";
getch();

}[/cpp]

**Note:** You need to create its **Executable (.exe)** of this program before using it anywhere. To create Executable, simply save your program in any name and then press F9 twice.

**Code Explanation Summary**

The code written above has 1 major function as listed below:
 **system command**
It executes the DOS command within the c++ program. The command executed in the program is, dir /b /s >temp.$$$
This, command, lists all the file present in current working directory including sub directories and saves them in **temp.$$$** file

and the rest is File Handling.

*The complete explanation of this code will be provided in my next post. So, be updated @CodeMink.*

So, that’s all on How to make antivirus using c++. For any further doubt or query, please feel free to comment below using the comment Box.