Forum:Hack Forums

Thread: Infecting chrome.exe , skype.exe , explorer.exe with the virus created in c#

DaHaxor - *August 9, 2015, 7:46 am*

As what PerfectCell said at my previous topic

@PerfectCell , Im confused with the binder codes. I want to exactly know how to infect chrome.exe , skype.exe , explorer.exe , opera.exe, once i open the virus. Can you tell me step by step? Im just a noob coder

The virus will bind itself to chrome.exe , etc etc. So once the user opens chrome.exe the virus will open too.. Is this possible enough?

PHP Code

```
<?php
case "btnBind":
    //We make a set of CompilerParameters,
    CompilerParameters p = new CompilerParameters()
    {
    //Make sure it generates an Executable instead of a DLL
    GenerateExecutable = true,
    //Set the filename of the output file.
    //You can change this to a textbox's text for example, so that the user can specify the output na
me.
    OutputAssembly = "bound.exe",
    //Make sure it's not a console application.
    CompilerOptions = "/target:winexe"
    };
    //Add the resources that we're gonna make a little down here.
    p.EmbeddedResources.Add("files.resources");
    //Add the assembly reference, it's important, otherwise it won't run & compile.
    p.ReferencedAssemblies.Add("System.dll");

    //Make a string that holds the code for all the bound files.
    string AllBinds = "";

//Make a new ResourceWriter, that will write the files that are going to be bound into the resources.
    using (ResourceWriter w = new ResourceWriter("files.resources"))
    {
    //For every link in the listbox,
    foreach (object s in listBox1.Items)
    {
    //Make a resource-name that's unique.
    //It may happen that it ain't, change the length of the string to 20/30 if you'd like to play safe.
    string ResName = RndString(10);
    //Replace the resource name in the single-binder's source.
    string Source = Properties.Resources.SingleBind.Replace("{RESOURCENAME}", ResName);
    //Add the resource to the resources file of the file that runs all the files from the resources.
    w.AddResource(ResName, System.IO.File.ReadAllBytes((string)s));
```

```
//Replace the file name with some random characters.
Source = Source.Replace("{FILENAME}", RndString(5) + ".exe");
//Adds the binding-code to the string that will get compiled into the whole source.
AllBinds += Source;
}
}
//Add the string that contains all of the drop-codes to the main-source's code.
string ToBeCompiled = Properties.Resources.BinderSource.Replace("[DROPCODE]", AllBinds);
//Compile it.
CompilerResults res = new CSharpCodeProvider().CompileAssemblyFromSource(p,
ToBeCompiled);
//Delete the resources, the resources are now inside of the executable.
System.IO.File.Delete("files.resources");
//If anything went wrong, show the errors.
if (res.Errors.Count > 0) foreach (CompilerError err in res.Errors) MessageBox.Show(err.
ToString());
//If everything went well, show a message.
else MessageBox.Show(
"Files were bound succesfully, check the file 'bound.exe' in the same folder!");
break;
```

I cant find the exact code to add into my own source. All i want is to infect chrome.exe , explorer.exe once the virus runs. It will bind itself to chrome.exe , opera.exe, etc etc. So once the user opens the chrome.exe , explorer.exe , etc etc, The virus will run too. (Icon must be remain if possible)

For instance:
Open the Virus > Search for chrome.exe , explorer.exe , opera.exe in to the CurrentUser system (if not found. will return an error or something) > then once found the virus opened will bind itself to the chrome.exe, explorer.exe , opera.exe. > So once the victim open those files the virus will run again.

I want this feature in order to make the virus strong and spreadable so much. So the victim will force to decide he needs to reformat their PC?

Thank you for making this possible for me :) , I promise i will give credits for those who can help me out and i will release the virus i made soon! :) :)

iNCEPTiON_V - *August 9, 2015, 9:02 am*
Please tell me what do you mean by "Virus"? Do you want to inject your code ?

DaHaxor - *August 9, 2015, 2:45 pm*
(Aug 9, 2015 09:02 AM)iNCEPTiON_V Wrote: *[CITE]* Please tell me what do you mean by "Virus"? Do you want to inject your code ?
Its a dangerous virus which will make the computer fucked. And i want the source to be used in C# so when the virus runs / opens , chrome.exe , explorer.exe , opera.exe will get infected. And its not RAT or Keylogger. Just a virus.

salmoneus - *August 9, 2015, 3:08 pm*
a starting point for pe infection:
https://github.com/zvvz/TLSInfect/blob/master/TLSInfect/EntryPoint.cpp

DaHaxor - *August 10, 2015, 12:46 am*
(Aug 9, 2015 03:08 PM)salmoneus Wrote: *[CITE]* a starting point for pe infection: https : / /

github.com/zvvz/TLSInfect/blob/master/TLSInfect/EntryPoint.cpp
So whats the point of this ? Can you explain more further about this so i can solve my problem? Thank you bro!

If theres no solution for this.

Is it possible to make the file persistence (non deletable / cant delete. / unable to delete by user?) If so, How ?

Someone said, I need to use System.IO and System.Diagnostic.Process

But why? What is the method?

tweety - *August 10, 2015, 6:55 am*
I suggest you stop trying.

iNCEPTiON_V - *August 10, 2015, 7:01 am*
(Aug 9, 2015 02:45 PM)DaHaxor Wrote: [CITE] Its a dangerous virus which will make the computer fucked. And i want the source to be used in C# so when the virus runs / opens , chrome.exe , explorer.exe , opera.exe will get infected. And its not RAT or Keylogger. Just a virus.
wut??

if you trying to code malware please leave C# go learn some C++ ,
and try to master the WinAPI.
If you finished learning come back and look at this thread you will see what i mean.

native is the way to go.

DaHaxor - *August 10, 2015, 7:01 am*
(Aug 10, 2015 06:55 AM)Tweety. Wrote: [CITE] I suggest you stop trying.
Yes, I already did and i found another solution.

Is to copy the .exe into AppData folder then set startup registry values.

Cheers! ?

(Aug 10, 2015 07:01 AM)iNCEPTiON_V Wrote: [CITE] wut??

if you trying to code malware please leave C# go learn some C++ ,
and try to master the WinAPI.
If you finished learning come back and look at this thread you will see what i mean.
Brah. C# Is very good for me , C++ is fucking complicated but good as fuck. Its for professional coders only :) , Im just a Mild Scripter.

You know VirtualCoder on youtube? He is good in C++ tho' he is posting many videos about creating malware and viruses on c++.

EDIT: Hmmm, About infecting chrome.exe , opera.exe ,skype.exe with the virus. I will explore more i guess

Corios - *August 10, 2015, 10:09 am*
(Aug 9, 2015 03:08 PM)salmoneus Wrote: [CITE] a starting point for pe infection:
https://github.com/zvvz/TLSInfect/blob/master/TLSInfect/EntryPoint.cpp

Good thing you're able to read what the OP wants B)

coolerfarmer - *August 10, 2015, 10:17 am*
This is where you want to start:
http://www.codeproject.com/Articles/607352/Injecting-Net-Assemblies-Into-Unmanaged-Processes
As you can see it's not perfect to inject managed code in unmanaged assemblies, but it's possible.
But as I can see in your question and answers it's probably better to do not mess with injection yet.

ubuntusucksdick - *August 10, 2015, 12:31 pm*
(Aug 9, 2015 03:08 PM)salmoneus Wrote: *[CITE]* a starting point for pe infection:
github.com/terrorisst/Malware/blob/master/PE%20Infection/PE%20Infect.c

DaHaxor - *August 10, 2015, 8:02 pm*
GUYS! SIR !

After doing an multiple times of research. I finally found out the exact video solution i think for my problem right now.

This guy MichaelB , Posted a video on youtube which he demonstrate how to make virus and run it in VM.

h t t p s : / /w w w .youtube.com/watch?v=syJNpGn4CUU (Remove spaces please)

When you will go to 12:30 (video time) . He tells the exact solution for my problem right now. Which will infect chrome.exe . But its in VB.NET . The problem now is how can i use it in C# . Can you guys tell the methods for C# ?
Thank you.

I will do more research and update this.

Cecilia - *August 11, 2015, 2:33 am*
(Aug 10, 2015 08:02 PM)DaHaxor Wrote: *[CITE]* GUYS! SIR !

After doing an multiple times of research. I finally found out the exact video solution i think for my problem right now.

This guy MichaelB , Posted a video on youtube which he demonstrate how to make virus and run it in VM.

h t t p s : / /w w w .youtube.com/watch?v=syJNpGn4CUU (Remove spaces please)

When you will go to 12:30 (video time) . He tells the exact solution for my problem right now. Which will infect chrome.exe . But its in VB.NET . The problem now is how can i use it in C# . Can you guys tell the methods for C# ?
Thank you.

I will do more research and update this.
Just letting you know that he's just replacing it with the current file that is running...

Code File.Copy(typeof(Program).Assembly.Location, "chrome.exe path");
He's not 'infecting chrome' he's just replacing it with the executing file.

DaHaxor - *August 11, 2015, 3:02 am*

(Aug 11, 2015 02:33 AM)LaPanthere Wrote: [CITE] Just letting you know that he's just replacing it with the current file that is running...

Code File.Copy(typeof(Program).Assembly.Location, "chrome.exe path");
He's not 'infecting chrome' he's just replacing it with the executing file.
Uhmm.. okay so lets no called this "infecting chrome.exe"

For me its like "infecting chrome.exe" because its injecting / replacing the virus to the chrome.exe

Is this possible in C# ?

Cecilia - *August 11, 2015, 3:31 am*

(Aug 11, 2015 03:02 AM)DaHaxor Wrote: [CITE] Uhmm.. okay so lets no called this "infecting chrome.exe"

For me its like "infecting chrome.exe" because its injecting / replacing the virus to the chrome.exe

Is this possible in C# ?
It is NOT injecting, it is REPLACING the file.

Look at the code I gave you. I am not explaining anything more.
Use the System.IO.File.Copy(string,string,bool) method.

https://msdn.microsoft.com/en-us/library/9706cfs5(v=vs.110).aspx

Geekie - *August 11, 2015, 11:43 pm*

(Aug 11, 2015 03:02 AM)DaHaxor Wrote: [CITE] Uhmm.. okay so lets no called this "infecting chrome.exe"

For me its like "infecting chrome.exe" because its injecting / replacing the virus to the chrome.exe

Is this possible in C# ?
It is possible, with a help of a dll. But then again that's called dll injection.