

Forum:[Hack Forums](#)

Thread: [My Builder & Stub are not detected but the Output \(keylogger\) is detected](#)

µnKn0wn_H4CK3r - June 5, 2010, 5:32 am

Hi!

I try to finish (FUD) my keylogger but I have one problem:

- Builder undetected (by Avira Antivir)
- Stub undetected (by Avira Antivir)
- Output (keylogger generated) detected (by Avira Antivir)

Avira find 4 Trojan/Dropper. I have got to remove 1 detection, now Avira find only 3 Trojan/Dropper (I have changed the assembly to HijackThis assembly, add fake code).

- What's the problem?
- What I have to do to FUD the output?

Thanks in advance!

GoldStar - June 5, 2010, 5:39 am

You can use the search first. 5 threads about this where posted before.

<https://hackforums.net/showthread.php?tid=431874>

µnKn0wn_H4CK3r - June 5, 2010, 8:07 am

(Jun 5, 2010 05:39 AM)Miharbi-DoNo Wrote: [\[CITE\]](#) You can use the search first. 5 threads about this where posted before.

<https://hackforums.net/showthread.php?tid=431874> Already done and it stays 4 Tr/Dropper.Gen ? .. ONLY this shit of Avira Antivir detects my output and no one detect my stub (junk code or not, bad/good FileSplit, bad/good solution name, bad/good icon).

But, what is EOF (End Of File) precisely?

Code FileOpen(1, Application.ExecutablePath, OpenMode.Binary, OpenAccess.Read, OpenShare.Shared)

```
text1 = Space(LOF(1))
FileGet(1, text1)
```

```
FileClose(1)
```

```
options = Split(text1, FileSplit)This is not EOF?
```

GoldStar - June 5, 2010, 8:10 am

(Jun 5, 2010 08:07 AM)BabyHack Wrote: [\[CITE\]](#) Already done

...

But, what is EOF (End Of File) precisely?

Code FileOpen(1, Application.ExecutablePath, OpenMode.Binary, OpenAccess.Read, OpenShare.Shared)

```
text1 = Space(LOF(1))
FileGet(1, text1)
FileClose(1)
options = Split(text1, FileSplit)This is not EOF?
Means its not already done. read it all, you will find alternatives of EOF (Number 5).
```

Threadlocks - June 5, 2010, 8:32 am

but it still need at end how its done help

xSilent - June 5, 2010, 8:38 am

PM me and I'll show you how to use deaths resource API

Beck - June 5, 2010, 8:45 am

(Jun 5, 2010 05:32 AM)BabyHack Wrote: [CITE](#) Hi!

I try to finish (FUD) my keylogger but I have one problem:

- Builder undetected (by Avira Antivir)
- Stub undetected (by Avira Antivir)
- Output (keylogger generated) detected (by Avira Antivir)

Avira find 4 Trojan/Dropper. I have got to remove 1 detection, now Avira find only 3 Trojan/Dropper (I have changed the assembly to HijackThis assembly, add fake code).

- What's the problem?
- What I have to do to FUD the output?

Thanks in advance!
Check out Deathaders' threads. They should help a bunch.

Threadlocks - June 5, 2010, 8:51 am

hey can i use code dom insted of eof

pr0t0typ3 - June 5, 2010, 10:02 am

Yes but comedom compiles a completly new file while eof just writes to an already compiled file

µnKn0wn_H4CK3r - June 5, 2010, 1:46 pm

I think [this is a good solution](#) but I don't know how to precisely do to write the resources...

If anybody can help me... Because I tried these solutions but they don't work:

```
Code 'Imports System.Text
'Imports Builder.ResourceWriter
```

```
WriteResource("OutPut.exe", Encoding.Default.GetBytes("Test" & FileSplit & "Test2"))
Code FileOpen(1, "OutPut.exe", OpenMode.Binary, OpenAccess.ReadWrite, OpenShare.Default)
```

```
FilePut(1, "Test String 1" & FileSplit & "Test String 2")
```

```
FileClose(1)
How use the module please ??
```

Threadlocks - June 5, 2010, 6:33 pm

if we pass eof as string to stub then how do we appened it

µnKn0wn_H4CK3r - June 5, 2010, 11:50 pm

(Jun 5, 2010 06:33 PM)zorataa Wrote: [\[CITE\]](#) if we pass eof as string to stub then how do we appened it! don't really understand what you said (I'm french)...

But I'd really like to know how to use this module ? !

The WriteResource function return a boolean, not a string or else (bytes...). And when I try any methods, it doesn't works (not write resources in the output.exe).

dayan - June 6, 2010, 6:48 am

Bump this up! I also hav the same prob with him

oRc - June 6, 2010, 7:02 am

Make a string:

```
Code dim buildstring as string = (filesplit & options1 & filesplit & options2)Convert to Bytes:
Code dim getbytes as byte() = encoding.default.getbytes(buildstring)Writhing to resources:
Code writeresource(application.startuppath & "\server.exe", getbytes)In your stub:
Code dim getbytes as byte() = readresource(application.executablepath())
dim getstring As string = encoding.default.getstring(getbytes)
Dim options() = Split(getstring, filesplit)
    options1 = options(1)
    options2 = options(2)
```

µnKn0wn_H4CK3r - June 6, 2010, 8:06 am

(Jun 6, 2010 07:02 AM)oRc Wrote: [\[CITE\]](#) Make a string:

```
Code dim buildstring as string = (filesplit & options1 & filesplit & options2)Convert to Bytes:
Code dim getbytes as byte() = encoding.default.getbytes(buildstring)Writhing to resources:
Code writeresource(application.startuppath & "\server.exe", getbytes)In your stub:
Code dim getbytes as byte() = readresource(application.executablepath())
dim getstring As string = encoding.default.getstring(getbytes)
Dim options() = Split(getstring, filesplit)
    options1 = options(1)
    options2 = options(2)I don't understand...
```

```
Code FileOpen(1, Application.StartupPath & "\Stub.exe", OpenMode.Binary, OpenAccess.Read,
OpenShare.Default)
```

```
Stub = Space(LOF(1))
FileGet(1, Stub)
```

```
FileClose(1)
```

```
Dim BuildString As String = Stub & FileSplit & TextBox1.Text & FileSplit & etc
Dim BuildBytes As Byte() = Encoding.Default.GetBytes(BuildString)
```

```
FileOpen(1, Application.StartupPath & "\" & "OutPut.exe", OpenMode.Binary,
OpenAccess.ReadWrite, OpenShare.Default)
```

```
WriteResource("OutPut.exe", BuildBytes)
```

```
FileClose(1)
```

It doesn't works !

Modesty - June 6, 2010, 8:08 am

Doesnt that mean the fact that its the stuff that is entered into the stub that makes it detected. If so, encrypt what u enter?

µnKn0wn_H4CK3r - June 6, 2010, 8:13 am

(Jun 6, 2010 08:08 AM)P Y R O Wrote: [\[CITE\]](#) Doesnt that mean the fact that its the stuff that is entered into the stub that makes it detected. If so, encrypt what u enter?But I want write the bytes in the output ("OutPut.exe")..

Actually, this code does nothing (don't write bytes).

µnKn0wn_H4CK3r - June 6, 2010, 12:19 pm

Bump...

Spoiler ([Click to View](#))TooShort & & Too Short.

µnKn0wn_H4CK3r - June 8, 2010, 8:27 am

Nobody...?

I really need this, please ? ...

pr0t0typ3 - June 8, 2010, 8:43 am

Then use the resource update api Deathader posted a nice example for it

µnKn0wn_H4CK3r - June 8, 2010, 8:49 am

(Jun 8, 2010 08:43 AM)pr0t0typ3 Wrote: [\[CITE\]](#) Then use the resource update api Deathader posted a nice example for itI understand nothing. But really nothing...

I'm a newbie and I'd like to learn & understand how to use it...

Resource update API?

Code <DllImport("kernel32.dll", SetLastError:=True)> _

Private Function UpdateResource(ByVal hUpdate As IntPtr, ByVal lpType As String, ByVal lpName As String, ByVal wLanguage As UShort, ByVal lpData As IntPtr, ByVal cbData As UInteger) As Boolean

End Function....

oRc - June 8, 2010, 9:23 am

Deathader didn't write tutorial in order to stop noob`s from copy pasta thing so they eventually give up.

newbie`s start`s here <http://www.homeandlearn.co.uk/net/vbnet.html>
not binder`s etc..