

Forum:[Hack Forums](#)

Thread: [\[FREE\] Most powerfull process protector \[Not killable by CMD or Taskmgr with admin\]](#)

TheExclusive - December 22, 2014, 6:27 am

[Excuse]

Sorry guys for my previous thread where i sold this source.
It was a stupid idea and i didn't knew i had to post it in marketplace.
I decide to give it away for free now.
PM me for the direct link of the project.

[Threat introduction]

There are a lot of process protector sources online.
I have seen some public sources that cause BSOD.
Or some that say's access denied when end process.
But they can easily be terminated or to suspicious.

[Process protector]

This process protector is so powerfull the taskmanager can't kill it even with admin rights.
I also tried to kill it with multiple script's but every time it fail to end the process.

[Scan]

[- 100% FUD source](#)

[Proof]

[img]<http://s7.postimg.org/61uk8jqfd/proof.gif>[/img]

Only tested with windows 7

ElementalTree - December 22, 2014, 6:36 am

Would be nice with a working "proof" image

SIM-2137258 - December 22, 2014, 6:44 am

I will pm me, your methods interest me thank you for sharing free :)

nathan72389 - December 22, 2014, 6:57 am

easily killed.
just freeze and end the process or send it a error message.

Only3 - December 22, 2014, 7:41 am

pm is worse then selling if u want to share post it else keep it private

TheExclusive - December 22, 2014, 7:45 am

(Dec 22, 2014 08:41 AM)Only3 Wrote: [\[CITE\]](#) pm is worse then selling if u want to share post it else keep it private

I thought it would be easy to have a project, so you can just compile and done.

(Dec 22, 2014 07:57 AM)nathan72389 Wrote: [\[CITE\]](#) easily killed.

just freeze and end the process or send it a error message.
A normal user can't kill this.
Can you learn me how to do this ?

0xfd - December 22, 2014, 8:02 am

pm me please, thank you for sharing free :)

Cookie.Monster - December 22, 2014, 8:07 am

Pmed you mate, could be nice to try out. :)

tweety - December 22, 2014, 8:46 am

(Dec 22, 2014 08:45 AM)TheExclusive Wrote: [\[CITE\]](#) I thought it would be easy to have a project, so you can just compile and done.

A normal user can't kill this.
Can you learn me how to do this ?

Odus - December 22, 2014, 9:42 am

False claims aside, you have no say in who you give this to since it isn't yours.

Code Imports System.Runtime.InteropServices

Public Class ProtectExecutable

Private Delegate Function VarPtrCallbackDelegate(ByVal address As Integer, ByVal unused1 As Integer, ByVal unused2 As Integer, ByVal unused3 As Integer) As Integer

Private Declare Function CallWindowProc Lib "user32" Alias "CallWindowProcA" (ByVal wndProc As VarPtrCallbackDelegate, ByRef var As Short, _
ByVal unused1 As Integer, ByVal unused2 As Integer, _
ByVal unused3 As Integer) As Integer

Private Declare Function CallWindowProc Lib "user32" Alias "CallWindowProcA" (ByVal wndProc As VarPtrCallbackDelegate, ByRef var As Integer, _
ByVal unused1 As Integer, ByVal unused2 As Integer, _
ByVal unused3 As Integer) As Integer

Private Shared Function VarPtrCallback(ByVal address As Integer, ByVal unused1 As Integer, ByVal unused2 As Integer, ByVal unused3 As Integer) As Integer
Return address
End Function

Private Shared Function VarPtr(ByRef var As Short) As Integer
Return CallWindowProc(AddressOf VarPtrCallback, var, 0, 0, 0)
End Function

Private Shared Function VarPtr(ByRef var As Integer) As Integer
Return CallWindowProc(AddressOf VarPtrCallback, var, 0, 0, 0)
End Function

<DllImport("Kernel32.dll")>

Private Shared Function GetCurrentProcess() As IntPtr
End Function

<DllImport("ntdll.dll")>

Private Shared Function ZwSetInformationProcess(ByVal _1 As IntPtr, ByVal _2 As IntPtr, ByVal _3 As IntPtr, ByVal _4 As IntPtr) As IntPtr

End Function

```
Public Shared Sub Main()  
    ZwSetInformationProcess(GetCurrentProcess(), &H21&, VarPtr(&H8000F129), &H4&)  
End Sub  
End Class
```

Only3 - December 22, 2014, 10:29 am

(Dec 22, 2014 10:42 AM)Odus Wrote: [\[CITE\]](#) False claims aside, you have no say in who you give this to since it isn't yours.

Code Imports System.Runtime.InteropServices

```
Public Class ProtectExecutable  
    Private Delegate Function VarPtrCallbackDelegate(ByVal address As Integer, ByVal unused1 As Integer, ByVal unused2 As Integer, ByVal unused3 As Integer) As Integer  
    Private Declare Function CallWindowProc Lib "user32" Alias "CallWindowProcA" (ByVal wndProc As VarPtrCallbackDelegate, ByVal var As Short, _  
        ByVal unused1 As Integer, ByVal unused2 As Integer, _  
        ByVal unused3 As Integer) As Integer  
    Private Declare Function CallWindowProc Lib "user32" Alias "CallWindowProcA" (ByVal wndProc As VarPtrCallbackDelegate, ByVal var As Integer, _  
        ByVal unused1 As Integer, ByVal unused2 As Integer, _  
        ByVal unused3 As Integer) As Integer  
    Private Shared Function VarPtrCallback(ByVal address As Integer, ByVal unused1 As Integer, ByVal unused2 As Integer, ByVal unused3 As Integer) As Integer  
        Return address  
    End Function  
    Private Shared Function VarPtr(ByVal var As Short) As Integer  
        Return CallWindowProc(AddressOf VarPtrCallback, var, 0, 0, 0)  
    End Function  
    Private Shared Function VarPtr(ByVal var As Integer) As Integer  
        Return CallWindowProc(AddressOf VarPtrCallback, var, 0, 0, 0)  
    End Function
```

```
<DllImport("Kernel32.dll")>
```

```
Private Shared Function GetCurrentProcess() As IntPtr  
End Function
```

```
<DllImport("ntdll.dll")>
```

```
Private Shared Function ZwSetInformationProcess(ByVal _1 As IntPtr, ByVal _2 As IntPtr, ByVal _3 As IntPtr, ByVal _4 As IntPtr) As IntPtr  
End Function
```

```
Public Shared Sub Main()  
    ZwSetInformationProcess(GetCurrentProcess(), &H21&, VarPtr(&H8000F129), &H4&)  
End Sub  
End Class
```

? this is based on vb6 code which u can find on net

Odus - December 22, 2014, 10:45 am

(Dec 22, 2014 11:29 AM)Only3 Wrote: [\[CITE\]](#) ? this is based on vb6 code which u can find on net That's what I was thinking. It's the same one OP tried to sell for \$10 in a previous thread.

Only3 - December 22, 2014, 11:06 am

(Dec 22, 2014 11:45 AM)Odus Wrote: [\[CITE\]](#) That's what I was thinking. It's the same one OP tried to sell for \$10 in a previous thread.

? well if its work i can agree with him good conversion ?

Odus - December 22, 2014, 11:16 am

(Dec 22, 2014 12:06 PM)Only3 Wrote: [\[CITE\]](#) ? well if its work i can agree with him good conversion ?

Really good conversion... Just not by him ?

Only3 - December 22, 2014, 11:38 am

(Dec 22, 2014 12:16 PM)Odus Wrote: [\[CITE\]](#) Really good conversion... Just not by him ?

? <https://fuckav.ru/showthread.php?t=18410> its early to decide that he copy it let wait for him

?MrRoot - December 23, 2014, 9:11 am

and what if you do Kill process tree?

Only3 - December 23, 2014, 9:22 am

for all that say it can be kill i try it by accident and needed to restart as i cant kill it even with process explorer

He B TeMy - December 23, 2014, 10:32 am

(Dec 23, 2014 10:22 AM)Only3 Wrote: [\[CITE\]](#) for all that say it can be kill i try it by accident and needed to restart as i cant kill it even with process explorer

I bet i can kill it with process explorer, just like i can kill eset with Process Hacker.

Edit: I got the code, i just never tested it..

CottleSilver - December 23, 2014, 11:32 am

Send pm with no response, can someone send me the link with the source?

Malware? - December 23, 2014, 12:02 pm

In process hacker, go to properties of the process and kill all of the threads

.cYRil. - December 23, 2014, 12:37 pm

Sounds like interesting wanna check this out

Malware? - December 23, 2014, 4:05 pm

Code Public Class ProtectProcessNew

Private Delegate Function VarPtrCallbackDelegate(ByVal address As Integer, ByVal unused1 As Integer, ByVal unused2 As Integer, ByVal unused3 As Integer) As Integer

<DllImport("ntdll.dll")>

Private Shared Function ZwSetInformationProcess(ByVal _1 As IntPtr, ByVal _2 As IntPtr, ByVal _3 As IntPtr, ByVal _4 As IntPtr) As IntPtr

End Function

<DllImport("user32.dll")>

Private Shared Function CallWindowProcA(ByVal wndProc As VarPtrCallbackDelegate, ByRef var As Integer, ByVal unused1 As Integer, ByVal unused2 As Integer, ByVal unused3 As Integer) As Integer

End Function

Private Shared Function VarPtrCallback(ByVal address As Integer, ByVal unused1 As Integer, ByVal unused2 As Integer, ByVal unused3 As Integer) As Integer

Return address

```

End Function
Public Shared Sub Protect()
    ZwSetInformationProcess(System.Diagnostics.Process.GetCurrentProcess().Handle, &H21&,
    CallWindowProcA(AddressOf VarPtrCallback, &H8000F129, 0, 0, 0), &H4&)
End Sub
End Class

```

CottleSilver - December 24, 2014, 12:18 am

Dose not work with windows 8 :) This is useless

TheExclusive - December 24, 2014, 9:55 am

(Dec 22, 2014 10:42 AM)Odus Wrote: [\[CITE\]](#) False claims aside, you have no say in who you give this to since it isn't yours.

```

Code Imports System.Runtime.InteropServices

Public Class ProtectExecutable
    Private Delegate Function VarPtrCallbackDelegate(ByVal address As Integer, ByVal unused1 As Integer, ByVal unused2 As Integer, ByVal unused3 As Integer) As Integer
    Private Declare Function CallWindowProc Lib "user32" Alias "CallWindowProcA" (ByVal wndProc As VarPtrCallbackDelegate, ByRef var As Short, _
        ByVal unused1 As Integer, ByVal unused2 As Integer, _
        ByVal unused3 As Integer) As Integer
    Private Declare Function CallWindowProc Lib "user32" Alias "CallWindowProcA" (ByVal wndProc As VarPtrCallbackDelegate, ByRef var As Integer, _
        ByVal unused1 As Integer, ByVal unused2 As Integer, _
        ByVal unused3 As Integer) As Integer
    Private Shared Function VarPtrCallback(ByVal address As Integer, ByVal unused1 As Integer, ByVal unused2 As Integer, ByVal unused3 As Integer) As Integer
        Return address
    End Function
    Private Shared Function VarPtr(ByRef var As Short) As Integer
        Return CallWindowProc(AddressOf VarPtrCallback, var, 0, 0, 0)
    End Function
    Private Shared Function VarPtr(ByRef var As Integer) As Integer
        Return CallWindowProc(AddressOf VarPtrCallback, var, 0, 0, 0)
    End Function

    <DllImport("Kernel32.dll")>
    Private Shared Function GetCurrentProcess() As IntPtr
    End Function

    <DllImport("ntdll.dll")>
    Private Shared Function ZwSetInformationProcess(ByVal _1 As IntPtr, ByVal _2 As IntPtr, ByVal _3 As IntPtr, ByVal _4 As IntPtr) As IntPtr
    End Function

    Public Shared Sub Main()
        ZwSetInformationProcess(GetCurrentProcess(), &H21&, VarPtr(&H8000F129), &H4&)
    End Sub
End Class

```

I never said i choose the one i send it to.

I have just send the direct link to every user that pmed me.

ali_m0000 - December 24, 2014, 5:32 pm

May I have the code please ?

I will pm u

Ooops I just discovered that I can't pm you
will you please pm me ?

nathan72389 - December 24, 2014, 6:12 pm

(Dec 24, 2014 06:32 PM)ali_m0000 Wrote: [\[CITE\]](#) May I have the code please ?

I will pm u

Ooops I just discovered that I can't pm you
will you please pm me ?

just signed up to leach something.

too bad you cant read because you would of seen that the code is posted in the post DIRECTLY
before yours.

CottleSilver - December 25, 2014, 2:45 am

Test on windows 8:

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

Menalix - December 25, 2014, 7:00 pm

Worst shit code.....

It's so easy preventing process from being killed anyways, just unlist it with
NtQuerySystemInformation hook.

nepHaXOr - May 28, 2015, 8:30 pm

Private me good method. Seems you are pro in this methods :D

AshleyUK - May 28, 2015, 8:57 pm

(May 28, 2015 08:30 PM)nepHaXOr Wrote: [\[CITE\]](#) Private me good method. Seems you are pro in
this methods :D

You do realize the last post was 5 months ago. The post also says to PM him not to grave dig.

SIM-2233573 - May 29, 2015, 2:28 am

Grave digging. Anyways, to share my opinion (and to up my post count), I've had more success with
cProtect.

hackforums.net/archive/index.php/thread-497391.html

I hope this will be the last message on this thread. Really shouldn't threads this old.

d4rkito - June 21, 2015, 6:42 pm

Can you pm me please? I'm not able to send pms yet.

Fat Autist12 - June 22, 2015, 2:08 am

Could i please get this download. Thanks in advance