

Forum:[Hack Forums](#)

Thread: [Undocumented Native APIs for Suspending Processes](#)

pr0t0typ3 - December 27, 2010, 4:07 am

Don't flame I know that I posted some code with a similar point some days ago.

I found this when I did some research about undocumented Functions in the ntdll Library

It is shorter then the other code.

Enjoy, give Credits and don't leech.

Code Module NTSuspendProcess

```
#Region "APIs"
  <DllImport("ntdll.dll")> _
  Private Function NtSuspendProcess(ByVal hHandle As IntPtr) As Boolean
  End Function
  <DllImport("ntdll.dll")> _
  Private Function NtResumeProcess(ByVal hHandle As IntPtr) As Boolean
  End Function
#End Region
Public Function SuspendProcess(ByVal ID As Integer) As Boolean
  Try
    Dim p As Process = Process.GetProcessById(ID)
    Return NtSuspendProcess(p.Handle)
  Catch ex As Exception
    Return False
  End Try
End Function
Public Function ResumeProcess(ByVal ID As Integer) As Boolean
  Try
    Dim p As Process = Process.GetProcessById(ID)
    Return NtResumeProcess(p.Handle)
  Catch ex As Exception
    Return False
  End Try
End Function
End Module
```

Navigator - December 27, 2010, 4:17 am

ntdll.dll is part of the Native API, not Windows API.

pr0t0typ3 - December 27, 2010, 4:20 am

(Dec 27, 2010 05:17 AM)Navigator Wrote: [\[CITE\]](#) ntdll.dll is part of the Native API, not Windows API.
Yeah my misstake. Thank you.

njq8 - December 27, 2010, 5:06 am

work on vista 32bit ^^

thanks very nice code

Neroxan - December 27, 2010, 7:45 pm

tehee... You .net kids really should look @ some of the vb6 runpe's every now and then. Nice cluebat for those who werent aware of it though.

affixiate - December 27, 2010, 8:33 pm

(Dec 27, 2010 08:45 PM)~WyldeChylde~ Wrote: [CITE](#) tehee... You .net kids really should look @ some of the vb6 runpe's every now and then. Nice cluebat for those who werent aware of it though. It really depends how you design it. I use the native functions for my C# RunPE.

It's quicker to call the ntdll import since most of the Windows APIs call something in ntdll to do the work. However, it also is uncertain. Microsoft explicitly tells you not to use many of the undocumented functions because they are well, undocumented, and can be altered at anytime.

Anyway, pr0t0typ3, solid work. If I could give rep here, I would give you some green apples.

d3c0mpil3r - December 27, 2010, 9:33 pm

Don't worry affixiate, +repped him from yours and my side :)

affixiate ([Click to View](#))Gave you too :)