

Forum:[Hack Forums](#)

Thread: [Anti Sandboxie and Anti VMWare](#)

thegodhello - January 31, 2015, 2:16 am

Looking for a AutoIT code to detect
if its in sandboxie,

i'd think about:

```
Code If _ProcessUser(@AutoItPID) <> @UserName Then MsgBox(0, "", "Running in sandboxie context")
```

```
Func _ProcessUser($iPid)
    Local Const $wbemFlagReturnImmediately = 0x10
    Local Const $wbemFlagForwardOnly = 0x20
    Local $userName = ""

    Local $objWMIService = ObjGet("winmgmts://./root/cimv2")
    Local $colPID = $objWMIService.ExecQuery("Select * from Win32_Process Where ProcessID = " & $iPid & "", "WQL", $wbemFlagReturnImmediately + $wbemFlagForwardOnly)
    For $objPID In $colPID
        If $objPID.ProcessID = $iPid Then
            $objPID.GetOwner($userName)
            ExitLoop
        EndIf
    Next

    Return $userName
EndFunc
```

thegodhello - February 2, 2015, 2:47 am

ing this up, need to know it

xx jasper

Unc3nZureD - February 2, 2015, 5:23 pm

Use this very simple source:

```
Code If WinGetText("Program Manager") = "0" Then Exit
```

French Products - February 4, 2015, 6:14 am

You can use this (is more short lol)

```
Quote:If ProcessExists("SbieCtrl.exe") Then Exit
```

Unc3nZureD - February 5, 2015, 3:55 pm

However my solution can prevent running not only in Sandboxie, but it can detect some other unknown sandboxes. Most of them restrict access to that window, so you can detect them :)

DuguWudi - March 24, 2015, 11:02 am

(Feb 5, 2015 04:55 PM)Unc3nZureD Wrote: [\[CITE\]](#) However my solution can prevent running not only in Sandboxie, but it can detect some other unknown sandboxes. Most of them restrict access to that window, so you can detect them :)

You mean such vm environment?

BTW, what happen to your autoit website?

Unc3nZureD - March 24, 2015, 3:24 pm

Quite a few people seemed to be active, so I abandoned the project. I had some other stuffs to do :) I started learning C/C++, RE and much other things :)

Nope, I mean that the following line:

Code If WinGetText("Program Manager") = "0" Then Exit

Can block other unknown sandboxes like antivirus auto-sandbox. Since there are quite a plenty of them, you can't easily find the process name or some weak point, but I'm sure that these sandboxes are blocking access to currently existing windows. On every system the Desktop has this text, called "Program Manager". If it's blocked, then we're running in a sandboxed (restricted) enviroment.

Exussit - May 6, 2015, 7:35 pm

It's generally not to hard to check if the program is being run in a VM or not. Use WMI to query the motherboard vendor, and most generic VM's will return a string of Microsoft Corporation as the vendor.. One easy way to tell for one's run under the Hyper-V.

labbepierre - February 21, 2017, 4:36 am

(Mar 24, 2015 03:24 PM)Unc3nZureD Wrote: [\[CITE\]](#) Quite a few people seemed to be active, so I abandoned the project. I had some other stuffs to do :) I started learning C/C++, RE and much other things :)

Nope, I mean that the following line:

Code If WinGetText("Program Manager") = "0" Then Exit

Can block other unknown sandboxes like antivirus auto-sandbox. Since there are quite a plenty of them, you can't easily find the process name or some weak point, but I'm sure that these sandboxes are blocking access to currently existing windows. On every system the Desktop has this text, called "Program Manager". If it's blocked, then we're running in a sandboxed (restricted) enviroment. Thank you for info . One question , how bypass virus total scan or other malware scan pls ?

Unc3nZureD - February 24, 2017, 9:52 am

(Feb 21, 2017 05:36 AM)labbepierre Wrote: [\[CITE\]](#) Thank you for info . One question , how bypass virus total scan or other malware scan pls ?

Just have a look at the crypter section. People in Autolt are usually trying to add some hardcore obfuscation to their code, splitting up & encrypting strings, renaming variables and a lot more.

labbepierre - March 12, 2017, 4:29 pm

(Feb 24, 2017 10:52 AM)Unc3nZureD Wrote: [\[CITE\]](#) Just have a look at the crypter section. People in Autolt are usually trying to add some hardcore obfuscation to their code, splitting up & encrypting strings, renaming variables and a lot more.Ok thank you i'll keep looking for a code

evelboy - January 11, 2018, 9:46 am

code is ~10 years old dont know if its still works

Code #include <Array.au3>

```

If _IsInSandbox() Then
    MsgBox(64,"","I'm in a Sandbox")
Else
    MsgBox(64,"","I'm NOT in a Sandbox")
EndIf
Func _IsInSandbox()
    $vUserName = @UserName
    $vComputerName = @ComputerName
    $vProductKey =
DecodeProductKey(RegRead("HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\Current
Version","DigitalProductID"))
    $vDriveSerial = DriveGetSerial("C:\")
    $vExeName = StringLeft(@ScriptName,StringLen(@ScriptName)-4) ;scriptname excluding .exe
    $vExePath = @ScriptDir & "\"

    #cs
    If GWser = "55274-339-6006333-22900" Then
        bFound = True
    End If
    #ce
    If $vProductKey = "55274-339-6006333-22900" Then
        Return True
    EndIf

    #cs
    If GWser = "76487-OEM-0065901-82986" Then
        bFound = True
    End If
    #ce
    If $vProductKey = "76487-OEM-0065901-82986" Then
        Return True
    EndIf

    #cs
    If Environ("computername") = "XPSP3" Then
        If Environ("username") = "Joe" Then
            bFound = True
        End If
    End If
    #ce
    If $vComputerName = "XPSP3" Then
        If $vUserName = "Joe" Then
            Return True
        EndIf
    EndIf

    #cs
    If Left(Environ("computername"), 10) = "NONE-DUSEZ" Then
        bFound = True
    End If
    #ce
    If StringLeft($vComputerName,10) = "NONE-DUSEZ" Then

```

```

    Return True
EndIf

#cs
If Left(Environ("computername"), 5) = "VMLOG" Then
    bFound = True
End If
#ce
If StringLeft($vComputerName,5) = "VMLOG" Then
    Return True
EndIf
#cs
If Environ("username") = "Sndbx" Then
    If GetDriveSerial() = 546811503 Then bFound = True 'Sandbox of unknown AV
End If
#ce
If $vUserName = "Sndbx" Then
    If $vDriveSerial = 546811503 Then
        Return True ;Sandbox of unknown AV
    EndIf
EndIf

#cs
If Environ("username") = "tester" Then
    If GetDriveSerial() = 800539777 Then bFound = True 'Sandbox of unknown AV found...
End If
#ce
If $vUserName = "tester" Then
    If $vDriveSerial = 800539777 Then
        Return True ;Sandbox of unknown AV
    EndIf
EndIf

#cs
If Environ("USERNAME") = "panda" Then
    If Environ("computername") = "AUTO" Then bFound = True 'Msgbox "Panda Sandbox
Detected"
End If
#ce
If $vUserName = "panda" Then
    If $vComputerName = "AUTO" Then
        Return True ;Panda Sandbox Detected
    EndIf
EndIf

#cs
If Environ("username") = "currentuser" Then bFound = True 'MsgBox "Norman Sandbox
Detected"
#ce
If $vUserName = "currentuser" Then
    Return True ;Norman Sandbox Detected
EndIf

```

```

#cs
If App.Path = "C:\\" Then
    If App.EXEName = "file" Then bFound = True 'MsgBox "Sunbelt Sandbox Detected"
    If App.EXEName = "Sample" Then bFound = True 'MsgBox "Anubis Sandbox Detected"
End If
#ce
If $vExePath = "C:\\" Then
    If $vExeName = "file" Then
        Return True ;Sunbelt Sandbox Detected
    ElseIf $vExeName = "Sample" Then
        Return True ;Anubis Sandbox Detected
    EndIf
EndIf

#cs
If GetModuleHandle("SbieDll.dll") Then bFound = True 'MsgBox "Sandboxie Detected"
#ce
If _GetModuleHandle("SbieDll.dll") = True Then
    Return True
EndIf
EndFunc
Func _GetModuleHandle($vDLL)
    $modHandle = DllCall("kernel32.dll", "long", "GetModuleHandle", "str", $vDLL)
    If IsArray($modHandle) Then
        If $modHandle[0] > 0 Then
            If _ArrayFindAll($modHandle,$vDLL) Then
                Return True
            EndIf
        Else
            SetError(-9)
            Return False
        EndIf
    Else
        SetError(-10)
        Return False
    EndIf
EndFunc
Func DecodeProductKey($BinaryDPID)
    Local $bKey[15]
    Local $sKey[29]
    Local $Digits[24]
    Local $Value = 0
    Local $hi = 0
    local $n = 0
    Local $i = 0
    Local $dlen = 29
    Local $slen = 15
    Local $Result

    $Digits = StringSplit("BCDFGHJKMPQRTVWXY2346789","")

    $binaryDPID = stringmid($binaryDPID,105,30)

```

```

For $i = 1 to 29 step 2
    $bKey[int($i / 2)] = dec(stringmid($binaryDPID,$i,2))
next

For $i = $dlen -1 To 0 Step -1
    If Mod(($i + 1), 6) = 0 Then
        $sKey[$i] = "-"
    Else
        $hi = 0
        For $n = $slen -1 To 0 Step -1
            $Value = Bitor(bitshift($hi ,- 8) , $bKey[$n])
            $bKey[$n] = int($Value / 24)
            $hi = mod($Value , 24)
        Next
        $sKey[$i] = $Digits[$hi +1]
    EndIf

Next
For $i = 0 To 28
    $Result = $Result & $sKey[$i]
Next

Return $Result
EndFunc

```