

Forum:[Hack Forums](#)

Thread: [\[VB.net\] Small 'MemoryEngine' for Duming and and Writing](#)

pr0t0typ3 - December 22, 2010, 2:43 am

A small 'MemoryEngine' for dumping and modifying a process memory.

The FullDump Function will dump the whole process to a byte array.

The PartDump Function will dump a part of the process within the address bounds you enter.

The WriteToAbsoluteAddress will write to a absolute address in memory (There is no guarantee that it is within the process memory region.) The Buffer paramter contains the data to write.

The WriteToDynamicAddress will write to a specific address that is calcualted using the following formula Baseaddress of the Process + Your Address = ReadAddress. The Buffer Paramter contains the data to write.

Give Credits and don't leech

Code Module MemoryEngine

#Region "Dumping"

Public Function FullDump(ByVal ID As Integer) As Byte()

Try

Dim p As Process = Process.GetProcessById(ID)

Dim data(p.MainModule.ModuleMemorySize - 1) As Byte

ReadProcessMemory(p.Handle, p.MainModule.BaseAddress, data, data.Length, 0)

Return data

Catch ex As Exception

Return Nothing

End Try

End Function

Public Function PartDump(ByVal ID As Integer, ByVal Address As Integer, ByVal lenght As Integer) As Byte()

Try

Dim p As Process = Process.GetProcessById(ID)

Dim data(lenght - 1) As Byte

ReadProcessMemory(p.Handle, New IntPtr(p.MainModule.BaseAddress.ToInt32 + Address), data, data.Length, 0)

Return data

Catch ex As Exception

Return Nothing

End Try

End Function

#End Region

#Region "Writing"

Public Function WriteToAbsoluteAddress(ByVal ID As Integer, ByVal Address As Integer, ByVal Buffer As Byte()) As Boolean

```

Try
    Dim p As Process = Process.GetProcessById(ID)
    Return WriteProcessMemory(p.Handle, New IntPtr(Address), Buffer, Buffer.Length,
IntPtr.Zero)
Catch ex As Exception
    Return False
End Try
End Function
Public Function WriteToDynamicAddress(ByVal ID As Integer, ByVal Address As Integer, ByVal
Buffer As Byte()) As Boolean
    Try
        Dim p As Process = Process.GetProcessById(ID)
        Return WriteProcessMemory(p.Handle, New IntPtr(p.MainModule.BaseAddress.ToInt32 +
Address), Buffer, Buffer.Length, IntPtr.Zero)
    Catch ex As Exception
        Return False
    End Try
End Function

#End Region
#Region "APIs"
<DllImportAttribute("kernel32.dll", EntryPoint:="ReadProcessMemory", SetLastError:=True)> _
Private Function ReadProcessMemory(<InAttribute()> ByVal hProcess As System.IntPtr,
<InAttribute()> ByVal lpBaseAddress As System.IntPtr, <Out()> ByVal lpBuffer As Byte(), ByVal
nSize As UInteger, <OutAttribute()> ByRef lpNumberOfBytesRead As UInteger) As
<System.Runtime.InteropServices.MarshalAsAttribute(System.Runtime.InteropServices.Unmanage
dType.Bool)> Boolean
End Function
<DllImportAttribute("kernel32.dll", EntryPoint:="ReadProcessMemory", SetLastError:=True)> _
Private Function WriteProcessMemory(<InAttribute()> ByVal hProcess As System.IntPtr,
<InAttribute()> ByVal lpBaseAddress As System.IntPtr, <Out()> ByVal lpBuffer As Byte(), ByVal
nSize As UInteger, <OutAttribute()> ByRef lpNumberOfBytesWritten As UInteger) As
<System.Runtime.InteropServices.MarshalAsAttribute(System.Runtime.InteropServices.Unmanage
dType.Bool)> Boolean
End Function
#End Region

End Module

```

The-One - December 22, 2010, 5:51 am

Thanks, I was looking for this :)

6e756c6c - December 22, 2010, 6:51 am

I never noticed the Process.MainModule.ModuleMemorySize property. Nice post Proto, thanks.

My Life - December 22, 2010, 6:56 am

Really great post pr0t0typ3 . At last someting new I see :)

pr0t0typ3 - December 22, 2010, 6:56 am

(Dec 22, 2010 07:51 AM)Aeonhack Wrote: [CITE](#) I never noticed the Process.MainModule.ModuleMemorySize property. Nice post Proto, thanks.

No Problem. I'm glad some of you like it. I made this when I tried to make my RunPE-Detector and so I found this nice property.

d3c0mpil3r - December 22, 2010, 6:58 am

Will take a look for sure.

Thanks proto. :)

pr0t0typ3 - December 22, 2010, 7:05 am

No Problem. I also found a way of Stealing Steam Password when I tried developing something new. The only bad thing is, that it only works if the current steam session was started with the password entered. Should I sell it ?

StarZ - December 22, 2010, 7:34 am

Proto;

Clear Steam Cache > Steal the pass on login > ??? > Profit?!?!</p>
</div>
<div data-bbox=

Process.MainModule.ModuleMemorySize property. Nice post Proto, thanks.
same here. good job posting.

SIM-99212 - December 27, 2010, 11:35 am

Code The WriteToDynamicAddress will write to a specific address that is calculated using the following formula Baseaddress of the Process + Your Address = ReadAddress. The Buffer Paramter contains the data to write.

Just out of curiosity, would the WriteToDynamicAddress work as a RunPE substitute?

Nice code BTW.

pr0t0typ3 - December 28, 2010, 1:57 am

(Dec 27, 2010 12:35 PM)jawatim Wrote: [\[CITE\]](#) Code The WriteToDynamicAddress will write to a specific address that is calculated using the following formula Baseaddress of the Process + Your Address = ReadAddress. The Buffer Paramter contains the data to write.

Just out of curiosity, would the WriteToDynamicAddress work as a RunPE substitute?

Nice code BTW.

You could use it as a part of a RunPE but there are many other things that need to be done, like Setting a new Thread Context etc.

RockYy - January 4, 2011, 9:03 am

Thanks proto. gonna look through it and if its too hard for me yet, I'll retry it later =)

The-One - January 5, 2011, 2:10 pm

Okey, I try to write it into a file like this:

```
Code Dim id As IntPtr = p.Id
    Dim bt As Byte() = FullDump(id)
    Dim fs As New FileStream("dump.exe", FileMode.Create, FileAccess.Write)
    For i = 0 To bt.Length - 1
        fs.WriteByte(bt(i))
    Next
    fs.Close()
```

But all it does is nothing, to a file.

pr0t0typ3 - January 6, 2011, 3:39 am

(Jan 5, 2011 03:10 PM)The-One Wrote: [\[CITE\]](#) Okey, I try to write it into a file like this:

```
Code Dim id As IntPtr = p.Id
    Dim bt As Byte() = FullDump(id)
    Dim fs As New FileStream("dump.exe", FileMode.Create, FileAccess.Write)
    For i = 0 To bt.Length - 1
        fs.WriteByte(bt(i))
    Next
    fs.Close()
```

But all it does is nothing, to a file.

The ID is a Integer not IntPtr

Why don't you use the much simpler IO.File.WriteAllBytes Function ?

Did you try debugging ? Is the Byte Array empty ?

Try to change the things above and test them and then tell me again.

The-One - January 6, 2011, 7:59 am

(Jan 6, 2011 04:39 AM)pr0t0typ3 Wrote: [\[CITE\]](#)

The ID is a Integer not Intptr

Why don't you use the much simpler IO.File.WriteAllBytes Function ?

Did you try debugging ? Is the Byte Array empty ?

Try to change the things above and test them and then tell me again.

Tried that all and doesn't work. The file starts at 0x0010, but it has to start at 0x0400.