

Forum:[Hack Forums](#)

Thread: [\[VB.Net\] Local/Remote TCP info from process](#) [\[Source\]](#)

The-One - June 4, 2011, 1:16 pm

Hey,

I never really intended to release it as I had some shit with this getting it to work. Though I had lots of help with this since I liked it more then WireShark and I got all the info I needed without searching.

I've used this for packet logging of: HWID applications, games and other things you will find out while using this.

Screenshot:

[img]<http://i.min.us/jcNZU2.png>[/img]

We are going to use iphlapi.dll (GetExtendedTcpTable) to get the information.

First, declare the API and some structures we need:

```
Code <DllImport("iphlpapi.dll", SetLastError:=True)> _
    Private Function GetExtendedTcpTable(ByVal pTcpTable As IntPtr, ByRef OutBufLen As Integer, ByVal sort As Boolean, ByVal ipVersion As Integer, ByVal tblClass As Integer, ByVal reserved As Integer) As UInteger
        End Function

    Private Structure tcprows
        Public LocalAddress As Integer
        Public LocalPort As Integer
        Public RemoteAddress As Integer
        Public RemotePort As Integer
        Public ProcessID As Integer
    End Structure

    Private Structure tcptable
        Public NumEntries As Integer
    End Structure
```

Now comes the most important function of this, the part where we get all the connections.

```
Code Private Function GetAllTcpConnections() As tcprows()
    Const NO_ERROR As Integer = 0
    Const IP_v4 As Integer = 2
    Dim tTable As tcprows() = Nothing
    Dim buffSize As Integer = 0
    GetExtendedTcpTable(IntPtr.Zero, buffSize, True, IP_v4, 5, 0)
    Dim buffTable As IntPtr = Marshal.AllocHGlobal(buffSize)
    Try
        If NO_ERROR <> GetExtendedTcpTable(buffTable, buffSize, True, IP_v4, 5, 0) Then
            Return Nothing
        End If
    End Try
```

```

Dim tab As tcptable = Marshal.PtrToStructure(buffTable, GetType(tcptable))
Dim rowPtr As IntPtr = CLng(buffTable) + Marshal.SizeOf(tab.NumEntries)
tTable = New tcprows(tab.NumEntries - 1) {}

```

```

Dim rowSize As Integer = Marshal.SizeOf(GetType(tcprows))
For i As Integer = 0 To tab.NumEntries - 1
    Dim tcpRow As tcprows = Marshal.PtrToStructure(rowPtr, GetType(tcprows))
    tTable(i) = tcpRow
    rowPtr = CInt(rowPtr) + rowSize
Next
Finally
    Marshal.FreeHGlobal(buffTable)
End Try
Return tTable
End Function

```

As I'm using a Command Application I made this:

```

Code Public Sub CheckProcess_Tcp(ByVal procname As String)
    Dim allTcpConns As tcprows() = GetAllTcpConnections()
    For Each row As tcprows In allTcpConns
        For Each p As Process In Process.GetProcessesByName(procname)
            If row.ProcessID = p.Id Then
                Console.ForegroundColor = ConsoleColor.White
                Console.WriteLine("Remote: " & tIP(row.RemoteAddress) & ":" & tPort(row.RemotePort) &
vbNewLine)
                Console.WriteLine("Local: " & tIP(row.LocalAddress) & ":" & tPort(row.LocalPort) & vbNewLine)
                Console.WriteLine("Process: " & procname & "(" & row.ProcessID & ")" & vbNewLine)
                Try
                    For Each pm As ProcessModule In p.Modules
                        If pm.FileName.Contains(procname) Then
                            Console.WriteLine("Location: " & pm.FileName() & vbNewLine)
                        Exit For
                    End If
                Next
                Catch
                    Console.WriteLine("Location: Error - 32 bit process could not been read" & vbNewLine)
                End Try
                Console.WriteLine("--" & vbNewLine)
            End If
        Next
    Next
End Sub

```

This will check if a row in the table contains the matched ID of the process we are looking for.

As you see there are some errors. We need to translate the port and IP.

```

Code Private Function tPort(ByVal port As Integer) As Integer
    Return ((port And &HFF) << 8 Or (port And &HFF00) >> 8)
End Function
Public Function tIP(ByVal LongIP As Double) As String
    Dim ByteIP(4) As String
    Dim x As Byte = Nothing

```

Dim IP As String

If LongIP < 4294967296.0# And LongIP >= 0 Then

ByteIP(0) = Fix(LongIP / (256 ^ 3))

ByteIP(1) = Fix(((LongIP - (ByteIP(0) * (256 ^ 3))) / (256 ^ 2)))

ByteIP(2) = Fix(((LongIP - (ByteIP(0) * (256 ^ 3)) - (ByteIP(1) * (256 ^ 2))) / 256))

ByteIP(3) = ((LongIP - (ByteIP(0) * (256 ^ 3)) - (ByteIP(1) * (256 ^ 2)) - (ByteIP(2) * 256)))

IP = ByteIP(3) & "." & ByteIP(2) & "." & ByteIP(1) & "." & ByteIP(0)

tlP = IP

Else

tlP = -1

End If

End Function

Enjoy, any questions can be asked below. I'd appreciate if you reply below :D

Apple - June 4, 2011, 1:32 pm

Now everybody will be able to get Leaf's IP it connects to :(

Could you upload the binaries? I don't feel like writing a program lol

The-One - June 4, 2011, 2:23 pm

(Jun 4, 2011 01:32 PM)Apple Wrote: [\[CITE\]](#) Now everybody will be able to get Leaf's IP it connects to :(

Could you upload the binaries? I don't feel like writing a program lol

VT:

<http://www.virustotal.com/file-scan/report.html?id=491cd0e3cd63f86ec439192c8e327030fdc20ad300741f8e786ce57c4fc333d6-1307222006>

<http://www.mediafire.com/?db6br1lnpb0nnlm>

Btw, I just saw a HUGE grammar fault. can must be want. /facepalm.

Modesty - June 4, 2011, 2:30 pm

(Jun 4, 2011 01:32 PM)Apple Wrote: [\[CITE\]](#) Now everybody will be able to get Leaf's IP it connects to :(

Could you upload the binaries? I don't feel like writing a program lol

What do you mean "now"?

You could already do that by going to:

(Jun 4, 2011 01:32 PM)Apple Wrote: [\[CITE\]](#) Now everybody will be able to get Leaf's IP it connects to :(

Could you upload the binaries? I don't feel like writing a program lol

What do you mean "now"?

You could already do that by going to:

The-One - June 4, 2011, 2:42 pm

(Jun 4, 2011 02:30 PM)Modesty Wrote: [\[CITE\]](#) What do you mean "now"?

You could already do that by going to:

[img]'https://gyazo.com/34944ba3df92e6fdeca23c0939a1750d.png[/img]

What do you mean "now"?

You could already do that by going to:

[img']<https://gyazo.com/34944ba3df92e6fdeca23c0939a1750d.png>[/img]

Though, thats only on Ultimate, not on other versions.

xSilent - June 4, 2011, 2:43 pm

(Jun 4, 2011 01:32 PM)Apple Wrote: [\[CITE\]](#) Now everybody will be able to get Leaf's IP it connects to :(

I really hope your being sarcastic.

Pulser - June 4, 2011, 3:04 pm

(Jun 4, 2011 01:32 PM)Apple Wrote: [\[CITE\]](#) Now everybody will be able to get Leaf's IP it connects to :(

Could you upload the binaries? I don't feel like writing a program lol

You could do that with an HTTP Debugger anyway.

The-One - June 4, 2011, 3:08 pm

(Jun 4, 2011 03:04 PM)Mr. Predictable Wrote: [\[CITE\]](#) You could do that with an HTTP Debugger anyway.

I'm sure there are some l33t anti's on this forum ?

Apple - June 4, 2011, 3:23 pm

Not everybody has knowledge of these types of programs and The-one has brought more attention to them. That's why I'm saying now people can get the IP. What I actually meant to say was now more people can get it.

The-One - June 4, 2011, 3:24 pm

(Jun 4, 2011 03:23 PM)Apple Wrote: [\[CITE\]](#) Not everybody has knowledge of these types of programs and The-one has brought more attention to them. That's why I'm saying now people can get the IP. What I actually meant to say was now more people can get it.

Btw Apple, No offense on my last reply to you.

Apple - June 4, 2011, 3:29 pm

(Jun 4, 2011 03:24 PM)The-One Wrote: [\[CITE\]](#) Btw Apple, No offense on my last reply to you. What post are you referring to? I don't see any that could potentially give offense to me.

ra1d - June 4, 2011, 3:32 pm

Really nice share dude.

Keep up the good work :)

Modesty - June 4, 2011, 3:34 pm

(Jun 4, 2011 02:42 PM)The-One Wrote: [\[CITE\]](#) Though, thats only on Ultimate, not on other versions. This is on home premium...

The-One - June 4, 2011, 4:20 pm

(Jun 4, 2011 03:34 PM)Modesty Wrote: [\[CITE\]](#) This is on home premium...

Yes and the older Windows versions, anyway people might find it useful to not have to spit though Wireshark.

(Jun 4, 2011 03:29 PM)Apple Wrote: [\[CITE\]](#) What post are you referring to? I don't see any that

could potentially give offense to me.

You said now everyone could get the IP of Leaf, then Mr. Predictable said you can use HTTP Debugger and I said: I'm sure there are some l33t anti's on this forum.

gifar_ucuL - *June 11, 2011, 11:41 am*

wow nice man can i have a source :)

The-One - *June 12, 2011, 10:15 am*

(Jun 11, 2011 11:41 AM)gifar_ucuL Wrote: [\[CITE\]](#) wow nice man can i have a source :)

Its already there, but I've PM'ed you a copy of it.