Reversing VB Crackme 2.0 Eternal Bliss
by Rhytm [Dread]

(This short tutorial was written in Wordpad)

Collecting Information

Hi people, welcome to this short tutorial on how to crack Eternal Bliss' second Visual Basic Crackme. Everyone ready ?? Then lets go !!
First read the included txt file, here is the most important part:

Find the correct hardcoded code in this CrackMe. I've disabled the __vbastrcomp breakpoint in Softice and have made sure that the code is not seen explicitly in SmartCheck or in Hexeditor.

Since this is more of a practice and taste of VB cracking, I'll give you a few hints:
1) In SmartCheck, although you will not see the REAL code, if you observe carefully, you will see how the real code is constructed.
2) It is possible to trace in Softice.

ok, lets try to reverse this program using Smartcheck only :))
Fire up smartcheck (be sure it is well configured) load the program and enter a dummy serial in the textfield..
Select the "Show Errors and Specific Events" in Smartcheck and take a good look, you'll notice this important info:

First these Strings:
116104
1141019911632
Some more here..
10511532

Next you'll notice that your serial is read number by number and after a while there are to "Val" functions with quite some numbers as parameter.

Analyzing the Info and Reversing the Target

For the people that don't know what the "Val" function is, read this example first:

```
Dim MyValue
MyValue = Val("2457")    ' Returns 2457.
MyValue = Val(" 2 45 7")    ' Returns 2457.
MyValue = Val("24 and 57")    ' Returns 24.
```

Everything clear now :) ok, we will need more info, either by using SoftICE or the "Show all Events" option in Smartcheck. Select the "Show all Options" and take a good look at the code around the two Val functions.
You'll notice the __vbaVarTstEq function. If you don't know what this function is read Eternal Bliss' essay on Visual Basic functions first. We now know the two numbers from the Val function get compared (You probably had guessed it before..).
Now take a good look at the string. 84 104 105 115 32 Do you see it !!!

It's the decimal notation for ascii codes :)))
Lets translate the decimal notation to a ascii notation (You can use BJanes and Eternal Bliss' new tool)..
You'll get "This " <-- Including the space after the "s"
okiedokie, lets start all over again enter the code "This " (without the "") check your smartcheck code and take a look at the last compare. By now you should have noticed the strings we found when collecting information are the same used in the compare..
I won't tell you anymore.. Try it out yourself, this is a great target to start with 8)
If you really really really can't solve it yourself scroll down a while for the correct answer :P

I like to thank Eternal Bliss for his great page on the web. Where Fravia+ gives all the theoretical information Eternal Bliss gives us the **BEST** page on the web with lots of bits and bytes to practice.

Also I like to great all the guys from #cracking4newbies #dread #faith2000 and #win32asm :))

I want to tell all the people reading this essay to **START REVERSING CRACKME'S THEMSELVES** since loads of crackmes on Eternal Bliss' site haven't been reversed yet :))
Feel free to send all your questions & comments to Rhytm@newmail.net

Bye !!!!
Rhytm, Hope to see you soon in #cracking4newbies

Couldn't you solve it yourself ?? Shame on you !! You haven't studied Eternal Bliss' tutorial **AND** haven't got enough patience/brains !! Go study and try yourself, it's fun and easy !!!

Answer: This is the correct code