The Camper Crew Solution To Muad'Dib's CrackMe 1.0

Another amazingly simple crackme, only absolute newbies should be reading this! Therefore this tutorial is aimed at the very newbies, so please don't be offended by reading this if you're not a very newbie. And please remember that I'm still a newbie so please don't criticise me too much.

Target: Maud'Dibs CrackMe v1.0 (http://crackmes.cjb.net)

Tools: W32Dasm
A hex editor of your choice

Cracking The Nags

First of all create a backup copy of mdcm1.exe and rename it mdcm1.w32 - remember, we can't modify an exe while it's loaded in W32Dasm. Follow the usual procedure, analyse the running program first, then analyse the disassembly. OK, we have two MessageBoxA nags to kill, one at startup and one on exit - each time it is the same nag. Load up mdcm1.w32 into W32Dasm and create a disassembly. The nag we want to disable has the caption "Please register!" and contains the following text "I want your money! Please send me $20 to get rid of this screen", so open up the String Data References window and have a look for both of those strings, you'll seem them both, so double click on the second string you see. You should see this:

```
/ / / / / / / / / / / / / / / / / / /   Dead Listing   / / / / / / / / / / / / / / / / / / / / / / / / /

Address     Machine Code                      Assembler Instructions

* Referenced by a CALL at Addresses:
|:00401208     , :00401254
|
:004012BF 6A00                              push 00000000                                      ; push ty
of MsgBox onto stack

* Possible StringData Ref from Data Obj ->"Please register!"                    ; title
                                                            |
:004012C1 682D304000                        push 0040302D                          ; push title onto stack

* Possible StringData Ref from Data Obj ->"I want your money!   Please send "       ; text
                                                                    ->"me $20 to get rid of this screen!"
                                                            |
:004012C6 683E304000                        push 0040303E                          ; push text onto stack
:004012CB 6A00                              push 00000000                          ; push handle of owner wnd to stack

* Reference To: USER32.MessageBoxA, Ord:01BBh
                                                            |
:004012CD E842000000                        Call 00401314                   ; call MessageBoxA

/ / / / / / / / / / / / / / / / / / /   Dead Listing   / / / / / / / / / / / / / / / / / / / / / / / / /
```

We can easily see what's going on by analysing this code. First of all W32Dasm shows us where this code snippet is being called from, you'll see it is called twice, and how many times is the nag called? Twice of course, 00401208 is the call at startup, 00401254 the call on exit. So from this we can deduct that there are two blindingly obvious ways to crack the crackme. We can nop the calls at 00401208 and 00401254, or we can nop the call to MessageBoxA shown above at 004012CD, and the push instructions above, otherwise we cause a GPF. I'll leave it up to you to decide which method you use, but maybe the former is the best because the amount of nops for the latter is 19, whereas it is 10 for the former, almost half as many.

A Section On Nopping For Those OF You Not In The Know

You can use any hex editor to do this, but I'll tell you how to use Hiew, a popular hex editor amongst beginners. For both methods we need to find out the offsets we need to patch, so if you're going to use the first method, we need two offsets. Press [Shift + F12] in W32Dasm and enter 00401208 into the box and click OK. The bar in W32Dasm should now be green, it is the number after @Offset which we're interested, so write it down (608h) you can omit the noughts. Now repeat the same for the second call @ 00401254 you should get (654h). Now open mdcm1.exe in Hiew and press [Return] twice and then [F5] and type 608 (without the h). You should see 10 digits, every two digits is one byte, so you have 5 bytes, and you have to nop these 5 bytes. The hex byte for nop is 90 so press [F3] and then type 90 5 times, press [F9], and then repeat for the second call, and [F10] to exit Hiew.

That's all folks

Greetz fly out to all those who've written great tutorials, tKC, Ed!son, LaZaRuS, Intern, R!SC, Quantico, and a hell of a lot more who I can't think of now. Hope you enjoyed and understood my poor effort of a tutorial.

Eddie Van Camper [The Camper Crew]
evc.campercrew@innocent.com
ICQ#: 43669548