

Security-Crack

GERMAN CRACKING FORCE / PC -ÄÄÄÜ

Cracking - HowTo #1 made for you by Yaan! [Laxity]

Due to countless requests, I will show you how to crack a shareware program.

The example i will be using is Ghosttyper 1.0e You can get it here:

www.ghosttyper.com.

If you want to crack it using this tutorial, be sure to get version 1.0e.

Otherwise, the adress-areas and patterns i will tell you about may be different.

Oke lets get started.

Things you will need:

*HEXEDITOR:

I`m using Ultraedit 5.20, because it has those c00l little tabs to switch between different files, and it has no size-limit. Any other HExEd will do the same.

If you have it, you can also use HIEW.

*DISASSEMBLER:

I`m still using WDASM 8.9, because i can`t unpack that damn IDA 3.75

You will find WDASM spread all over the net.

*PC

If you are reading this on a monitor, THAT problem is solved already.

*BRAIN

Oke, this one`s really easy, so you won`t need a high IQ.

Now let`s get into it:

First, let`s install that proggy and take a look. To keep this usable for all you guys out there, i will translate the german stuff into english. (If there is some)

Now, let`s see what has been installed:

GhostKey.dll -----> Dynamic Link Library

Ghostt_e.hlp -----> Helpfile_English

Ghostt_g.hlp -----> Helpfile_German

GhostTyp.exe -----> Executable

GhostTyp.INI -----> .INI

Install.log -----> This one logged the installation

Now let`s run the .EXE to see how the program is protected and what it does to make you register. There we have a SplashScreen, saying that the program is not registered, and that you are in the 30-day TrialPeriod. The "OK" button is not active until a TimeLoop is done. Now, click on "Register" and type in your name and a code-dummy. I use Yaan! [Laxity] for the name and 123456789 for the code. Click on "OK". There will be a message telling you that you have entered the wrong code. Write down that errormessage. We will use that to try to find out more about the protection. Let`s disassemble the .EXE with WDASM. Once it is

disassembled, you will see the program in ASM-code.

In WDASM, click on "String references" and search for the error message that popped up when you entered the wrong code. Did you find it ? No ?

Hmmmmmm. It`s not in there. Oke, that was shit. Normally, this is the first thing for me to do. When you can`t find it, you have to find & use a different AttackPoint to crack it.

Then lets peek a little bit into those string references to find something interesting.

Whooops. Wait. One string says "Unregistered". Thats bad, lets see if we find "Registered"

That`s what we want it to be, right ? Scroll a bit upwards and there you go.

DoubleClick on "Registered" once. I`m always doing another DoubleClick to see if there`s another Reference for that one. Now you are into the code where the program

decides if it is registered or not. So lets see :

* Referenced by a (U)nconditional or (C)onditional Jump at Address:

| :00462FA3(C)

|

:00463012 E891D9FBFF call 004209A8

:00463017 8B45FC mov eax, dword ptr [ebp-04]

:0046301A E8C53EFAFF call 00406EE4

:0046301F 8BF0 mov esi, eax

:00463021 E86A8CFFFF call 0045BC90

```
:00463026 3BF0 cmp esi, eax
```

```
:00463028 754E jne 00463078 <----- Hello there !
```

```
:0046302A E89D8BFFFF call 0045BBCC
```

```
:0046302F 6A00 push 00000000
```

```
:00463031 8D4DF4 lea ecx, dword ptr [ebp-0C]
```

```
* Possible StringData Ref from Code Obj ->"Registered"
```

This is what you should see after you DoubleClicked on "Registered". As you can see

at the top, this StringData is referenced by a conditional jump at address :00462FA3.

So we are doing a rude "dirty" crack for now, take a look at the above asm code.

There are some calls you can step into by clicking "Goto code location" This will tell you more about what is done. But to me, this area seems to be important:

```
:00463026 3BF0 cmp esi, eax -----> compares esi / eax
```

```
:00463028 754E jne 00463078 -----> Jumps to 00463078 if Not Equal
```

So it looks like if the code you entered is compared to the right one calculated,

and he jumps to 00463078, if it`s not the correct one. Hmmmmm. So why don`t we simply

change the conditional jump ? Let`s make him jump only to 00463078 (bad register),

if you entered the CORRECT code. So we will have an any Name / Number Crack.

Every Number will register the program, except the correct one which is calculated by

the protection scheme.

In WDASM, click on this line:

```
:00463028 754E jne 00463078
```

At the statusline, you will see the offset where you can patch the jump into the GhostTyp.exe. For me, it says @offset 00062428h. So bring up your HexEditor and load the .exe. Go to offset 00062428h

You will find the following pattern:

```
->75<- 4E E8 9D 8B FF FF 6A uNè•<ÿÿj
```

now change the 75 at the beginning to 74:

```
->74<- 4E E8 9D 8B FF FF 6A tNè•<ÿÿj
```

Changing the 75 to 74 will replace the JNE with JE in line 00463028

So it will jump only if the code is correct (Jump if Equal)

I will refer to some byt patterns later.

Save the patched file under a different name (e.g. GhostTypCRK.exe)

Let`s see if it worked. Run GhostTypCRK.exe, click on "Registrieren"

(that`s "Register" in german), enter any Name and any Number, click on "OK"

Wheeee. You are registered, and you just cracked Ghosttyper 1.0e

(Thanks to this tutorial, don`t forget) So now you can go for your own

cracks and practice some years & join Laxity !

Now, I have a little surprise for you: Ghosttyper has a built-in keygenerator !

After you have cracked & registered the program, look at your GhostTyp.INI.

Did you ? There you have THE CORRECT CODE with the name you entered.

And it`s not even crypted. Doh; that`s realllllly stupid !

To generate more numbers, simply delete the .INI and register as often as you like.

THATSIT !

Sure, there are more ways to crack it, and this one`s not the cleanest, but it works and is easy to explain in this way.

*Bytepatterns:

JNE Jump if Not Equal 75

JE Jump if Equal 74

JMP Jump EB

NOP No Operation 90

JA Jump if Above 77

JB Jump if Below 72

JNA Jump if Not Above 76

JLE Jump if Less or Equal 7E

JL Jump if Less 7C

You HAVE to learn assembler to crack programs. Oke, you will NEED the basics, but the more you know about ASM, the faster you can understand the code & protection. (Oh, really ?)

○ ○

° Raptor #1 (driver) PC Ü °

○ ○

○ ○

○ ○

○ ○

⁰ Are you a courier?... Contact the founder and ask him if you can join! ⁰

0 0

[Back home](#)



More Categories

FREE-BANNERS.COM

Page updated u

