

Forum:[Hack Forums](#)

Thread: [\[Tutorial\] Cracking applications with HWID \[PATCHING\]](#)

The-One - January 13, 2011, 7:08 am

Hey,

Okey, so most of you know how to crack applications, you can use different methods, I preffer using a disassembler like OllyDbg.

But, we can also use other tools, like the tools I will be using.

So, get your program you want to crack and start reading!

Step 1:

Download the following files:

- [Simple Assembly Explorer](#)
- [Red Gate Reflector .NET](#)

Step 2:

Open the file you want to crack in Red Gate's reflector. (Drag it inside the form).

Now you will see one of these two icons:

[img]http://www.pl0xy.eu/images/32432kjxas3.png[/img]

Step 2b:

Open up Simple Assembly Explorer en navigate to the folder where u saved the executable you want to crack.

Right click, and click Deobfuscator. You will see a window, if you haven't already, I recommend using this setting(There might be better one's, if you have one, make a screen and post it, and I will edit it):

[img]http://www.pl0xy.eu/images/19238123.png[/img]

Now, for the next step, use the deobfuscated file (Saved in the directory where the original file is saved with the same name but .Deobf added at the end).

Step 3:

Now, if you want the source first or find something (Maybe the link where the program gets the return of the hwid check?) right click on the executable and click reflector.

If you want to patch(crack) it, right click and press class editor.

Step 4:

Follow the steps on the picture:

[img]http://www.pl0xy.eu/images/4u34kj.png[/img]

I selected the string, so it searches for a string (Because the link is set as a string), then I select the string I want to search for, easy, 'http:/' (If that doesn't work try 'www' , or 'hwid', 'check' etc. If you really can't find it, you can try getting it with [Sandboxie](#) with sandboxie you can see what link the program navigates to.) then we click next to let it search.

Step 5:

[img]http://www.pl0xy.eu/images/23219312.png[/img]

If you want to know what this does:

Spoiler ([Click to View](#))Code 1 -

- 2 - Stack the string 'Checking..' to a string
- 3 - Set the string to SetLoggerText.Text
- 4 - A link to the webpage
- 5 -
- 6 - Get whats in Textbox1 (Your hwid)
- 7 - Temporary saves it to use it
- 8 - Add the link + hwid
- 9 -
- 10 -
- 11 - Create a new request (With the link + hwid)
- 12 - Get the request (= Passed, or not)

Now, right click on the link, and select edit. You will see the link in a textbox. Open the link in a browser and (Don't enter a GUID) and see what it returns.(SAVE IT)

Step 6:

Open notepad.

Paste in the found string and save it as a .php (Name doesn't matter)

Upload it on a host.

Step 7:

Next, open the Simple Assembly Explorer window again, and replace the following part IN the TEXTBOX.

Lets say I found: <http://www.url.com/hwid.php?hwid=>

Replace: <http://www.url.com/hwid.php> with <http://www.yoursite.com/yourphp.php>

Press OK.

Step 8:

Now, at Simple Assembly Explorer's menubar, press save, save the patched file.
Open it, and you will see it now logs in!

This was my tutorial.
Enjoy, for questions, reply.

lexx13 - January 13, 2011, 7:20 am

Nice tutorial man. Thanks for the release.

The-One - January 13, 2011, 7:27 am

(Jan 13, 2011 08:20 AM)lexx13 Wrote: [\[CITE\]](#) Nice tutorial man. Thanks for the release.
Thanks for the reply! Enjoy. ?

[eno] - January 13, 2011, 7:30 am

Very, very helpful, layout and writing easy to understand.
I like this, hope you success always.
peace :)

DeathStar™ - January 13, 2011, 7:34 am

Good, Just straight to the point. And you've just learned the leeching users of worlds biggest leeching forum how to leech even more :)
But srsly Great tut!

The-One - January 13, 2011, 7:36 am

Thanks you both, hoping to see more reply's, Enjoy!

Burnzy - January 13, 2011, 7:41 am

thanks! I hope it will work i got few apps to crack :D

maniek191 - January 13, 2011, 7:42 am

Nice tutorial man. Thanks for the release.

The-One - January 13, 2011, 7:46 am

(Jan 13, 2011 08:41 AM)mladen190 Wrote: [\[CITE\]](#) thanks! I hope it will work i got few apps to crack :D
Good luck sir.

(Jan 13, 2011 08:42 AM)maniek191 Wrote: [\[CITE\]](#) Nice tutorial man. Thanks for the release.
No problem :D

wisd0m - January 13, 2011, 7:48 am

Detailed tutorial, you put some effort in.

Good share mate.

FEL1X. - January 13, 2011, 7:48 am

Very basic tut. Thanks.

^^

The-One - January 13, 2011, 7:50 am

(Jan 13, 2011 08:48 AM)wisd0m Wrote: [\[CITE\]](#) Detailed tutorial, you put some effort in.

Good share mate.

Thanks, like how you can see that. ?

fredde_jason - January 13, 2011, 7:52 am

This is cool! What you should do is a tutorial on how to protect your app from this sort of reversing.

Ghostenigma - January 13, 2011, 7:55 am

I like it.Very good tutorial..I'll test it later;)

My Life - January 13, 2011, 7:56 am

A great tutorial I must say . Enjoy it very much :)

Keep it up . I want more :P

The-One - January 13, 2011, 7:58 am

Thanks all ^ , I will maybe make more later on.

FEL1X. - January 13, 2011, 8:00 am

(Jan 13, 2011 08:52 AM)fredde_jason Wrote: [\[CITE\]](#) This is cool! What you should do is a tutorial on how to protect your app from this sort of reversing.

add encryption algoritms for your sites and other PRIVATE informations

fredde_jason - January 13, 2011, 8:01 am

(Jan 13, 2011 09:00 AM)fel1x Wrote: [\[CITE\]](#) add encryption algoritms for your sites and other PRIVATE informations

Ofcourse, but they can still access your source code, and that is not very good.

The-One - January 13, 2011, 8:04 am

(Jan 13, 2011 09:01 AM)fredde_jason Wrote: [\[CITE\]](#) Ofcourse, but they can still access your source code, and that is not very good.

Yes, but there are several ways of protecting it, just look around on this section.

fredde_jason - January 13, 2011, 8:11 am

(Jan 13, 2011 09:04 AM)The-One Wrote: [\[CITE\]](#) Yes, but there are several ways of protecting it, just look around on this section.

Yeah, but you just showed how to reverse that protection! Any suggestions?

FEL1X. - January 13, 2011, 8:15 am

(Jan 13, 2011 09:11 AM)fredde_jason Wrote: [\[CITE\]](#) Yeah, but you just showed how to reverse that protection! Any suggestions?

EVERTHING can be cracked. So if your app is popular it will be cracked soon. There is no lifetime protection.

The-One - January 13, 2011, 8:23 am

(Jan 13, 2011 09:15 AM)fel1x Wrote: [\[CITE\]](#) EVERYTHING can be cracked. So if your app is popular it will be cracked soon. There is no lifetime protection.

And 'nuff said, you can only make it hard to crack, or annoying to crack. ?

nickjonnes - January 13, 2011, 8:48 am

nice tut thanks!

but...

what if it has been obfuscated with smart assembly 5
.net reflector cant remove that?
cheers nick

The-One - January 13, 2011, 8:49 am

(Jan 13, 2011 09:48 AM)nickjonnes Wrote: [\[CITE\]](#) nice tut thanks!
but...
what if it has been obfuscated with smart assembly 5
.net reflector cant remove that?
cheers nick
But Smart Assembly Explorer can ;)

nickjonnes - January 13, 2011, 9:01 am

(Jan 13, 2011 09:49 AM)The-One Wrote: [\[CITE\]](#) But Smart Assembly Explorer can ;)oh thanks bro
when was it updated last time i check it could do this but then again that was a very long time ago
thanks again
nick

The-One - January 13, 2011, 9:04 am

(Jan 13, 2011 10:01 AM)nickjonnes Wrote: [\[CITE\]](#) oh thanks bro
when was it updated last time i check it could do this but then again that was a very long time ago
thanks again
nick
No problem, enjoy and good luck.

fredde_jason - January 13, 2011, 9:25 am

(Jan 13, 2011 09:23 AM)The-One Wrote: [\[CITE\]](#) And 'nuff said, you can only make it hard to crack, or
annoying to crack. ?
Well, how do you do that? ;)

d3v1l401 - January 13, 2011, 10:06 am

an excellent tutorial,thanks mate i'll try it!

unsurpassable - January 13, 2011, 10:09 am

Very nice tut! Thanks for sharing!

The-One - January 13, 2011, 10:09 am

(Jan 13, 2011 11:06 AM)d3v1l401 Wrote: [\[CITE\]](#) an excellent tutorial,thanks mate i'll try it!
No problemo.

(Jan 13, 2011 10:25 AM)fredde_jason Wrote: [\[CITE\]](#) Well, how do you do that? ;)
Encrypt it, add dead ending jumps, just junk it. But not those junk generator's make junk INSIDE a
code.

Darkfader - January 13, 2011, 10:11 am

Very nice tutorial there dude. But its too easy to block cracking process(not permanently but make it
almost impossible)
I know one program with very good protection and it shut your computer down when ever you try to
read it in any debugger. I dont say its impossible to crack that program but it really is hard as hell.

SIM-209986 - January 13, 2011, 10:13 am

This is not even cracking -.-

Darkfader - January 13, 2011, 10:16 am

(Jan 13, 2011 11:13 AM)MaXim Wrote: [\[CITE\]](#) This is not even cracking -.-

Quote:Software cracking is the modification of software to remove or disable features which are considered undesirable by the person cracking the software, usually related to protection methods: copy protection, trial/demo version, serial number, hardware key, date checks, CD check or software annoyances like nag screens and adware

Isn't it? wikipedia knows ;)

SIM-209986 - January 13, 2011, 10:19 am

(Jan 13, 2011 11:16 AM)Darkfader Wrote: [\[CITE\]](#) Quote:Software cracking is the modification of software to remove or disable features which are considered undesirable by the person cracking the software, usually related to protection methods: copy protection, trial/demo version, serial number, hardware key, date checks, CD check or software annoyances like nag screens and adware

Isn't it? wikipedia knows ;)

it is patching. not the same as cracking.

Rs6 - January 13, 2011, 10:26 am

Thanks for the share buddy.

The-One - January 13, 2011, 11:22 am

Thank you all, yea no program is uncrackable.

(Jan 13, 2011 11:19 AM)MaXim Wrote: [\[CITE\]](#) Isn't it? wikipedia knows ;)

it is patching. not the same as cracking.

[/quote]

Cracking a safe -> Blow up the lock. (remove it)

Cracking a program -> Make the protection fail. (remove it)

S!rk0 - January 13, 2011, 11:32 am

If for that reson i obfuscate my program and set aan anti for Simple Assambly Explorer :p

The-One - January 13, 2011, 11:50 am

(Jan 13, 2011 12:32 PM)S!rk0 Wrote: [\[CITE\]](#) If for that reson i obfuscate my program and set aan anti for Simple Assambly Explorer :p

No, thats not possible. You have to do it another way (A way I don't know)

n31ght0 - July 17, 2011, 6:26 pm

search i google and found this great tutorial.

but i cant see the images. can you re-upload that ?

thanks ?

envious.` - May 23, 2012, 2:24 am

Thanks for the tutorial but can you please fix the images! :)

hoocrax - May 23, 2012, 2:47 am

(May 23, 2012 02:24 AM)ATI™ Wrote: [\[CITE\]](#) Thanks for the tutorial but can you please fix the images! :)

This thread is like 1 year 4 months old ? But the OP seems to have been online recently ?

So try pm'ing him ?

The-One - *May 23, 2012, 3:04 am*

I don't have the images anymore.

~Closed.